Buchberger-Zacharias Theory of Multivariate Ore Extensions

Michela Ceria
DISI
Università di Trento
michela.ceria@unitn.it

Teo Mora
DIMA
Università di Genova
theomora@disi.unige.it

December 27, 2018

Abstract

We present Buchberger Theory and Algorithm of Gröbner bases for multivariate Ore extensions of rings presented as modules over a principal ideal domain. The algorithms are based on Möller Lifting Theorem.

In her 1978 Bachelor's thesis [54] Zacharias discussed how to extend Buchberger Theory [7, 8, 10] from the case of polynomial rings over a field to that of polynomials over a Noetherian ring with suitable effectiveness conditions.

In the meantime a similar task was performed in a series of papers — Kandri-Rody–Kapur [21] merged the rewriting rules behind Euclidean Algorithm with Buchberger's rewriting, proposing a Buchberger Theory for polynomial rings over Euclidean domains; Pan [40] studied Buchberger Theory for polynomial rings over domains introducing the notions of strong/weak Gröbner bases — which culminated with [35].

Such unsorpassed paper, reformulating and improving Zacharias' intuition, gave efficient solutions to compute both weak and strong Gröbner bases for polynomial rings over each Zacharias ring, with particolar attention to the PIR case. Its main contribution is the reformulation of Buchberger test/completion ("a basis F is Gröbner if and only if each S-polynomial between two elements of F reduces to 0") in the more flexible *lifting theorem* ("a basis F is Gröbner if and only if each element in a minimal basis of the syzygies among the leading monomials lifts, via Buchberger reduction, to a syzygy among the elements of F"). The only further contribution to this ultimate paper is the survey [6] of Möller's results which reformulated them in terms of Szekeres Theory [51].

The suggestion of extending Buchberger Theory to non-commutative rings which satisfy Poincaré-Birkhoff-Witt Theorem was put forward by Bergman [5], effectively applied by Apel–Lassner [3, 4] to Lie algebras and further extended to solvable polynomial rings [22, 23], skew polynomial rings [16, 17, 18] and to other algebras [1, 11, 26, 27] which satisfy Poincaré-Birkhoff-Witt Theorem and thus, under the standard interpretation of Buchberger Theory in terms of filtration/graduations [2, 30, 33, 50, 29, 12], have the classical polynomial ring as associated graded rings.

In particular Weispfenning [53] adapted his results to a generalization of the Ore extension [39] proposed by Tamari [52]; then Weispfenning's construction was generalized by his student Pesch [41, 42], introducing the notion of *iterative Ore extension with commuting variables*

$$\mathsf{R} := R[Y_1; \alpha_1, \delta_1][Y_2; \alpha_2, \delta_2] \cdots [Y_n; \alpha_n, \delta_n],\ R \text{ a domain;}$$

the concept has been called *Ore algebra* in [13] and is renamed here as *multivariate Ore extension* (for a different and promising approach to Ore algebras see [24]).

Bergman's approach and most of all extensions are formulated for rings which are vector spaces over a field; in our knowledge the only instances in which the coefficient ring R is presented as a $\mathbb{D}$-module over a domain $\mathbb{D}$ (or at least as a $\mathbb{Z}$-module) are Pritchard's [43, 44] extension of Möller Lifting Theory to non-commutative free algebras and Reinert's [45, 46] deep study of Buchberger Theory on Function Rings.

Following the recent survey on Buchberger-Zacharias Theory for monoid rings $R[\mathsf{S}]$ over a unitary effective ring R and an effective monoid S [32], we propose here a Möller–Pritchard lifting theorem presentation of Buchberger-Zacharias Theory and related Gröbner basis computation algorithms for multivariate Ore extensions. The twist w.r.t. [32] is that there $R[\mathsf{S}]$ coincides with its associated graded ring; here R, its associated graded ring

$$G(\mathsf{R}) := R[Y_1; \alpha_1][Y_2; \alpha_2] \cdots [Y_n; \alpha_n]$$

and the commutative polynomial ring $R[Y_1, \cdots, Y_n]$ coincide as sets and as left R-modules, but, as rings, they have different multiplications.

We begin by recalling Ore's original theory [39] of non-commutative polynomials $R[Y]$, relaxing the original assumption that R is a field to the case in which R is a domain (Section 1.1) and Pesch's constructions of multivariate Ore extensions (Section 1.2) and graded multivariate Ore extensions (Section 1.3), focusing on the arithmetics of the main Example 14

$$\mathsf{R} := R[Y_1; \alpha_1][Y_2; \alpha_2] \cdots [Y_n; \alpha_n], R := \mathbb{Z}[x] \quad \alpha_i(x) := c_i x^{e_i}, c_i \in \mathbb{Z} \setminus \{0\}, e_i \in \mathbb{N} \setminus \{0\}.$$

Next, we introduce Buchberger Theory in multivariate Ore extensions recalling the notion of term-orderings (Section 2.1), definition and main properties of left, right, bilateral and restricted Gröbner bases (Section 2.2) and Buchberger Algorithm for computing canonical forms in the case in which R is a skew field (Section 2.3).

We adapt to our setting Szekeres Theory [51] (Section 3), Zacharias canonical representation with related algorithm (Section 4) and Möller Lifting Theorem (Section 5).

The next Sections are the algorithmic core of the paper: we reformulate for multivariate Ore extensions over a Zacharias ring R

- Möller's algorithm for computing the required Gebauer–Möller set (*id est* the minimal basis of the module of the syzygies among the leading monomials) for Buchberger test/completion of left weak bases (Section 6.1);
- Möller's reformulation, requiring only l.c.m. computation in R for the case in which R is a (Zacharias) PID (Section 6.2) or a (Zacharias) PIR (Section A);

– still in the case in which R is a PID (Section 6.3) or a PIR (Section A), Möller's completion of a left weak basis to a left strong one;

– Gebauer–Möller criteria [19] for producing a Gebauer–Möller set (Section 6.4);

– Kandri-Rody–Weispfenning completion [22] of a left weak basis for producing a bilateral one (Section 7.1);

– Weispfenning's [53] restricted completion (Section 7.2);

– as a technical tool required by Weispfenning's restricted completion, how to produce right Gebauer–Möller sets (Section 7.3).

Finally, we reverse to a theoretical survey summarizing the structural theorem for the case in which R is a Zacharias PID (Section 8), specializing to our setting Spear's Theorem [49, 29] (Section 9) and extending to it Lazard's Structural Theorem [25] (Section 10).

In an appendix we discuss, as far as it is possible, how to extend this theory and algorithms to the case in which R is a PIR (Section A).

1 Recalls on Ore Theory

1.1 Ore Extensions

Let R be a not necessarily commutative domain; Ore [39] investigated under which conditions the (left) R-module $\mathsf{R} := R[Y]$ of all the *formal polynomials is made a ring* under the assumption *that the multiplication of polynomials shall be associative and both-sided distributive* and the limitation imposed by the postulate that *the degree of a product shall be equal to the sum of the degree of the factors.*

It is clear that, due to the distributive property, given two "monomials" bY^r, $aY^s \in \mathsf{R}$, $a, b \in R$, it suffices to define the product $bY^r \cdot aY^s \in \mathsf{R}$ or even more specifically, to define the product $Y \cdot r, r \in R$; this necessarily requires the existence of maps $\alpha, \delta : R \to R$ such that

$$Y \cdot r = \alpha(r)Y + \delta(r) \text{ for each } r \in R;$$

Ore calls $\alpha(r)$ the *conjugate* and $\delta(r)$ the *derivative* of r.

Under the required postulate clearly we have

1. for each $r \in R$, $\alpha(r) = 0 \implies r = 0$,

so that α is injective.

It is moreover sufficient to consider, for each $r, r' \in R$, the relations

$$\alpha(r + r')Y + \delta(r + r') = Y \cdot (r + r') = Y \cdot r + Y \cdot r' = (\alpha(r) + \alpha(r'))Y + \delta(r) + \delta(r'),$$

$$\alpha(rr')Y + \delta(rr') = Y \cdot (rr') = (Y \cdot r) \cdot r' = \alpha(r)\alpha(r')Y + \alpha(r)\delta(r') + \delta(r)r',$$

and, if R is a skew field, and $r \neq 0$,

$$Y = (Y \cdot r) \cdot r^{-1} = \alpha(r)\alpha(r^{-1})Y + \alpha(r)\delta(r^{-1}) + \delta(r)r^{-1},$$

to deduce that

2. α is a ring endomorphism;
3. the following conditions are equivalent:
   (a) for each $d \in R \setminus \{0\}$ exists $c \in R \setminus \{0\} : Y \cdot c = dY + \delta(c), \alpha(c) = d$;
   (b) α is a ring automorphism;
4. δ is an α-derivation of R *id est* an additive map satisfying[1]
$$\delta(rr') = \alpha(r)\delta(r') + \delta(r)r' \text{ for each } r, r' \in R;$$
5. if R is a skew field, then each $r \in R \setminus \{0\}$ satisfies
$$\alpha(r^{-1}) = (\alpha(r))^{-1}, \quad \delta(r^{-1}) = -(\alpha(r))^{-1}\delta(r)r^{-1};$$
6. $Im(\alpha) \subset R$ is a subring, which is an isomorphic copy of R;
7. $R_1 := \{r \in R : r = \alpha(r)\} \subset R$ is a ring, the *invariant ring* of R;
8. $R_0 := \{r \in R : \delta(r) = 0\} \subset R$ is a ring, the *constant ring* of R;
9. $\{r \in R : Y \cdot r = rY\} = R_0 \cap R_1$.
10. If R is a skew field, such are also $Im(\alpha)$, R_1 and R_0.
11. Denoting $Z := \{z \in R : zr = rz \text{ for each } r \in R\}$ the *center* of R, we have
$$\{r \in R : f \cdot r = rf \text{ for each } f \in \mathsf{R}\} = R_0 \cap R_1 \cap Z.$$

Moreover, if we consider two polynomials $f(Y), g(Y) \in \mathsf{R} \setminus \{0\}$,

$$f = aY^m + f_0, g = bY^n + g_0, a, b \in R \setminus \{0\}, m, n \in \mathbb{N}, f_0, g_0 \in \mathsf{R}, \deg(f_0) < m, \deg(g_0) < n,$$

we have
$$f \cdot g = a\alpha^m(b)Y^{m+n} + h(Y), \deg(h) < m + n;$$
since α is injective, $b \neq 0 \implies \alpha(b) \neq 0 \implies \alpha^m(b) \neq 0$ and since R is a domain it holds $\alpha^m(b) \neq 0 \neq a \implies a\alpha^m(b) \neq 0 \implies f \cdot g \neq 0$. As a consequence

12. R is a domain.

Definition 1. R with the ring structure described by conditions 1, 2, 4 above is called an *Ore extension* and is denoted $R[Y; \alpha, \delta]$.

Remark 2 (Ore). In an Ore extension $R[Y; \alpha, \delta]$, denoting $\mathcal{S} = \langle \alpha, \delta \rangle$ the free semigroup over the alphabet $\{\alpha, \delta\}$ and, for each $d \in \mathbb{N}$ and $i \in \mathbb{N}, 0 \leq i \leq d$, $\mathcal{S}_{d,i}$ the set of the $\binom{d}{i}$ words in $\mathcal{S}$ of length d in which occur i instances of α and $d - i$ instances of δ in an arbitrary order, we have
$$Y^d \cdot r = \sum_{i=0}^{d} \sum_{\tau \in \mathcal{S}_{d,i}} \tau(r)Y^i$$

[1] Whence, setting $r = r' = 1$, $\delta(1) = 0$.

for each $d \in \mathbb{N}$; for instance

$$\begin{aligned} Y^3 \cdot r &= \alpha^3(r)Y^3 + \delta^3(r) \\ &+ \left(\alpha^2\delta(r) + \alpha\delta\alpha(r) + \delta\alpha^2(r)\right) Y^2 \\ &+ \left(\alpha\delta^2(r) + \delta\alpha\delta(r) + \delta^2\alpha(r)\right) Y. \end{aligned}$$

In particular, for $f(Y) = \sum_{i=0}^{n} a_i Y^{n-i}$ and $g(Y) = \sum_{i=0}^{m} b_i Y^{m-i}$ in R we have

$$g(Y)f(Y) = \sum_{i=0}^{n+m} c_i Y^{n+m-i} \text{ with } c_0 = b_0\alpha^m(a_0) \text{ and } c_i = \sum_{\mathsf{a}=0}^{i} b_{\mathsf{a}} \sum_{\mathsf{b}=0}^{i-\mathsf{a}} \sum_{\tau \in \mathcal{S}_{m-\mathsf{a},i-\mathsf{a}-\mathsf{b}}} \tau(a_{\mathsf{b}}).$$

Remark 3 (Ore). Under the assumption that α is an automorphism (*cf.* 3.), each polynomial $\sum_{i=1}^{n} a_i Y^i \in \mathsf{R}$ can be uniquely represented as $\sum_{i=1}^{n} Y^i \bar{a}_i$ for proper values $\bar{a}_i \in R$.

In fact we have $ax = x\alpha^{-1}(a) - \delta(\alpha^{-1}(a))$ from which we can deduce inductively proper expressions

$$ax^n = x^n\alpha^{-n}(a) + \sum_{i=1}^{n} (-1)^i x^{n-i}\sigma_{in}(a),$$

for $\sigma_{in}(a) \in R$, properly defined (similarly to what done for $\tau \in \mathcal{S}_{d,i}$, but using the derivative and the inverse of the conjugate [39]).

□

1.2 Multivariate Ore Extensions

Let R be a not necessarily commutative domain.

Definition 4. An *iterative Ore extension* is a ring (whose multiplication we denote $\star$) defined as

$$\mathsf{R} := R[Y_1; \alpha_1, \delta_1][Y_2; \alpha_2, \delta_2] \cdots [Y_n; \alpha_n, \delta_n]$$

where, for each $i > 1$, α_i is an endomorphism and δ_i an α_i-derivation of the iterative Ore extension

$$R_{i-1} := R[Y_1; \alpha_1, \delta_1] \cdots [Y_{i-1}; \alpha_{i-1}, \delta_{i-1}].$$

As proved by Pesch in [41], it is possible to extend α_i to an endomorphism of R and δ_i to an α_i-derivation in R, by setting $\alpha_i(Y_j) = Y_j$ and $\delta_i(Y_j) = 0$ for each $i \leq j \leq n$.

A *multivariate Ore extension* (or: *Ore algebra* [13]; or: *iterative Ore extension with commuting variables* [41, 42]) is an iterative Ore extension which satisfies

- $\alpha_j\delta_i = \delta_i\alpha_j$, for each i, j, $i \neq j$,
- $\alpha_i\alpha_j = \alpha_j\alpha_i$, $\delta_i\delta_j = \delta_j\delta_i$ for $i < j \leq n$,
- $\alpha_j(Y_i) = Y_i, \delta_j(Y_i) = 0$ for $i \leq j \leq n$.

Lemma 5 (Pesch)**.** *In an iterative Ore extension, for each $i < j$ it holds*

$$Y_j \star Y_i = Y_iY_j \iff \alpha_j(Y_i) = Y_i, \delta_j(Y_i) = 0.$$

Proof. For each $i < j$, we have $Y_j \star Y_i = \alpha_j(Y_i)Y_j + \delta_j(Y_i)$. □

Since in this paper we are interested in iterative Ore extensions for which $Y_j \star Y_i = Y_iY_j$, by the previous Lemma 5, we can say that the maps α_i, δ_i are relevant only on the elements of R, so sometimes we will restrict them to R.

Lemma 6 (Pesch)**.** *An iterative Ore extension is a multivariate Ore extension iff $Y_j \star Y_i = Y_iY_j$ for each $i < j$.*

Proof. In fact, using Lemma 5 for each $r \in R$, we have

$$\begin{aligned} Y_j \star Y_i \star r &= Y_j \star (\alpha_i(r)Y_i + \delta_i(r)) \\ &= \alpha_j(\alpha_i(r)Y_i + \delta_i(r))\, Y_j + \delta_j(\alpha_i(r)Y_i + \delta_i(r)) \\ &= \alpha_j\alpha_i(r)Y_iY_j + \alpha_j\delta_i(r)Y_j + \delta_j(\alpha_i(r)Y_i) + \delta_j\delta_i(r) \\ &= \alpha_j\alpha_i(r)Y_iY_j + \alpha_j\delta_i(r)Y_j + \delta_j\alpha_i(r)Y_i + \delta_j\delta_i(r) \end{aligned}$$

and (by symmetry)

$$\begin{aligned} Y_iY_j \star r &= Y_i \star (\alpha_j(r)Y_j + \delta_j(r)) \\ &= \alpha_i\alpha_j(r)Y_iY_j + \delta_i\alpha_j(r)Y_j + \alpha_i\delta_j(r)Y_i + \delta_i\delta_j(r). \end{aligned}$$

□

Thus the R-module structure of a multivariate Ore extension can be identified with that of the polynomial ring $R[Y_1, \dots, Y_n]$ over its natural R-basis

$$\mathcal{T} := \{Y_1^{a_1} \cdots Y_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\}, \quad \mathsf{R} \cong R[\mathcal{T}] = \mathrm{Span}_R\{\mathcal{T}\}.$$

We can therefore denote $\alpha_{Y_i} := \alpha_i, \delta_{Y_i} := \delta_i$ for each i and, iteratively,

$$\alpha_{\tau Y_i} := \alpha_\tau\alpha_i, \delta_{\tau Y_i} := \delta_\tau\delta_i, \text{ for each } \tau \in \mathcal{T}.$$

Remark that a multivariate Ore extension is *not* an algebra; in fact, if we define, for $\tau = Y_1^{d_1} \cdots Y_n^{d_n}$ and $t = Y_1^{e_1} \cdots Y_n^{e_n}$ such that $\tau \mid t$

$$\binom{t}{\tau} := \binom{e_1}{d_1} \cdots \binom{e_n}{d_n},$$

we have

$$t \star r = \alpha_t(r)t + \sum_{\substack{\tau \in \mathcal{T} \\ \tau \mid t, \tau \neq t}} \binom{t}{\tau} \delta_{\frac{t}{\tau}} \alpha_\tau(r)\tau, \text{ for each } t \in \mathcal{T} \text{ and } r \in R.$$

We can define, for each $t \in \mathcal{T}$, a map

$$\theta_t : R \to \mathsf{R}, \quad \theta_t(r) = \sum_{\substack{\tau \in \mathcal{T} \\ \tau \mid t, \tau \neq t}} \binom{t}{\tau} \delta_{\frac{t}{\tau}} \alpha_\tau(r)\tau,$$

so that $t \star r = \alpha_t(r)t + \theta_t(r)$ for each $t \in \mathcal{T}$ and each $r \in R$.

Such maps α_t and θ_t satisfy properties analogous of those of Ore's conjugate and derivative:

Lemma 7. *With the present notation, for each $t \in \mathcal{T}$, we have*

1. *for each $r \in R$, $\alpha_t(r) = 0 \implies r = 0$,*
2. *α_t is a ring endomorphism;*
3. *the following conditions are equivalent:*
   (a) *for each $d \in R \setminus \{0\}$ exists $c \in R \setminus \{0\} : Y \star c = dY + \theta_t(c), \alpha_t(c) = d$;*
   (b) *α_t is a ring automorphism;*
4. *θ_t is an α_t-derivation of R;*
5. *if R is a skew field, then each $r \in R \setminus \{0\}$ satisfies*

$$\alpha_t(r^{-1}) = (\alpha_t(r))^{-1}, \quad \theta_t(r^{-1}) = -(\alpha_t(r))^{-1}\,\theta_t(r)r^{-1};$$

6. *$Im(\alpha_t) \subset R$ is a subring, which is an isomorphic copy of R.*

We further have

7. *if each α_i is an automorphism, also each α_t, $t \in \mathcal{T}$, is such.* □

1.3 Associated graded Ore Extension

Following the notation of 1.2 we give the following

Definition 8. A multivariate Ore extension

$$R[Y_1; \alpha_1, \delta_1][Y_2; \alpha_2, \delta_2] \cdots [Y_n; \alpha_n, \delta_n]$$

where each δ_i is zero, will be called a *graded Ore extension* (or: *Ore extension with zero derivations* [41, 42]) and will be denoted

$$\mathsf{R} := R[Y_1; \alpha_1][Y_2; \alpha_2] \cdots [Y_n; \alpha_n].$$

□

Lemma 9. *In a multivariate graded Ore extension,*

- *since it is an Ore algebra, the αs commute,*
- *and $t \star r = \alpha_t(r)t$ for each $t \in \mathcal{T}$ and $r \in R$.*

Remark 10. Note that, since multivariate Ore extensions coincide, as left R-modules, with the classical polynomial rings $R[Y_1, \ldots, Y_n]$ and so have the same R-basis, namely $\mathcal{T}$, they can share with the polynomial rings their standard $\mathcal{T}$-valuation [51, 30, 2, 33] [31, §24.4,24.6]. This justifies the definition below.

Definition 11. Given an Ore extension $\mathsf{R} := R[Y_1; \alpha_1, \delta_1][Y_2; \alpha_2, \delta_2] \cdots [Y_n; \alpha_n, \delta_n]$ the corresponding graded Ore extension $G(\mathsf{R}) := R[Y_1; \alpha_1][Y_2; \alpha_2] \cdots [Y_n; \alpha_n]$ is called its *associated graded Ore extension*. □

Example 12.

1. The first non obvious example of Ore extension was proposed in 1948 by D.Tamari [52] in connection with the notion of "order of irregularity" introduced by Ore in [38]; it consists of the graded Ore extension

$$\mathsf{R} := R[Y;\alpha],\ R = \mathbb{Q}[x] \text{ where } \alpha : R \to R : x \mapsto x^2.$$

2. Such construction was generalized by Weispfenning [53] who introduced the rings

$$\mathsf{R} := R[Y;\alpha],\ R = \mathbb{Q}[x] \text{ where } \alpha : R \to R : x \mapsto x^e,\ e \in \mathbb{N}$$

3. and extended by Pesch [41] to his *iterated Ore extensions with power substitution*

$$\mathsf{R} := R[Y_1;\alpha_1][Y_2;\alpha_2]\cdots[Y_n;\alpha_n],\ R = \mathbb{Q}[x]$$

where $\alpha_i : R \to R : x \mapsto x^{e_i},\ e_i \in \mathbb{N}$.

4. An Ore extension where α is invertible is discussed in [28]:

$$\mathsf{R} := R[S;\alpha], R = \mathbb{Q}[D_1, D_2, D_3]$$

where

$$\alpha : R \to R : f(D_1, D_2, D_3) \mapsto f(D_2 + 2D_1, D_3, -D_1)$$

whose inverse is

$$\alpha^{-1} : R \to R : f(D_1, D_2, D_3) \mapsto f(-D_3, D_1 + 2D_3, D_2).$$

□

Note that, while as R-modules R and $G(\mathsf{R})$ coincide both with the polynomial ring $\mathcal{P} = R[Y_1, \ldots, Y_n]$, the three rings have, in general, different arithmetics; we will denote $\star$ the multiplication of R and $*$ those of $G(\mathsf{R})$.

Example 13. The ring of Example 12.1.

$$\mathsf{R} := R[Y;\alpha],\ R = \mathbb{Q}[x] \text{ where } \alpha : R \to R : x \mapsto x^2$$

is an Ore extension which is graded.

Since the map

$$\delta : \mathbb{Q}[x] \to \mathbb{Q}[x] : x^i \mapsto \sum_{h=i}^{2i-1} x^h$$

is an α-derivation, $\mathsf{S} := R[Y;\alpha,\delta]$ is an Ore extension of which R is the associated graded Ore extension. □

In the following example, we define a nontrivial class of algebras, which will be used to illustrate our theory and algorithms.

Example 14. Since in Buchberger-Zacharias Theory, from an algorithmic point of view, one is interested only on the associated graded rings and thus the rôle of derivates is irrelevant, we illustrate the results for the Ore extensions with the zero-derivatives

$$\mathsf{R} := R[Y_1;\alpha_1][Y_2;\alpha_2]\cdots[Y_n;\alpha_n],\ R = \mathbb{Z}[x],$$

with $\alpha_i(x) := c_i x^{e_i}, c_i \in \mathbb{Z}\setminus\{0\}, e_i \in \mathbb{N}\setminus\{0\}$.

If we denote γ the map

$$\gamma : \mathbb{N}\times\mathbb{N}\setminus\{0\} \to \mathbb{N}, (a,e) \mapsto \sum_{i=0}^{a-1} e^i = \frac{1-e^a}{1-e}$$

where the last equality holds for $e \neq 1$, we have $Y_i^a * x^b = c_i^{b\gamma(a,e_i)} x^{e_i^a b} Y_i^a$.

Note that

$$\gamma(b,e) + e^b\gamma(a,e) = \sum_{i=0}^{b-1} e^i + \sum_{i=0}^{a-1} e^{b+i} = \sum_{i=0}^{a+b-1} e^i = \gamma(a+b,e). \tag{1-a}$$

Since $\alpha_j(\alpha_i(x)) = c_i\alpha_j(x^{e_i}) = c_i c_j^{e_i} x^{e_i e_j}$ and $\alpha_i(\alpha_j(x)) = c_j\alpha_i(x^{e_j}) = c_j c_i^{e_j} x^{e_i e_j}$, then R is a graded Ore extension if and only if

$$c_i c_j^{e_i} x^{e_i e_j} = \alpha_j(\alpha_i(x)) = \alpha_i(\alpha_j(x)) = c_j\alpha_i(x^{e_j}) = c_j c_i^{e_j} x^{e_i e_j}$$

id est

$$c_j^{e_i-1} = c_i^{e_j-1}. \tag{1-b}$$

We thus have $\binom{n}{2}$ relations among the n coefficients c_i. In particular we need to partition the indices as

$$\{1,\dots,n\} = E \sqcup O \sqcup S, E = \{i : 2 \mid e_i\}, O = \{i : 2 \nmid e_i > 1\}, S = \{i : e_i = 1\}.$$

If $I := O \sqcup E = \emptyset$ then each such equations are the trivial equality $1 = 1$ and thus all c_i are free. The situation is completely different when $I := O \sqcup E \neq \emptyset$; in fact,

- for $i \in S$ necessarily $c_i = \pm 1$;
- if a prime p divides at least a $c_j, j \in I$, then it divides each $c_i, i \in I$.

As regards the sign of c_i we can say that

- if $E \neq \emptyset$ then
  - c_i is positive for each $i \in S \cup O$,
  - the sign of $c_i, i \in E$, is undetermined but all the $c_i, i \in E$, have the same sign;
- if $E = \emptyset$ then the sign of $c_i, i \in S \cup O$ is undetermined.

For instance

– for $e_1 = e_4 = 1, e_2 = 5, e_3 = 3$ we have $S = \{1, 4\}, O = \{2, 3\}, E = \emptyset$ and

$$c_1^4 = c_2^0, c_1^2 = c_3^0, c_1^0 = c_4^0, c_2^2 = c_3^4, c_2^0 = c_4^4, c_3^0 = c_4^2,$$

whence $c_1 = \pm 1, c_4 = \pm 1, c_2 = \pm c_3^2$;

– for $e_1 = e_4 = 1, e_2 = 2, e_3 = 3$ we have $S = \{1, 4\}, O = \{3\}, E = \{2\}$, and

$$c_1 = c_2^0, c_1^2 = c_3^0, c_1^0 = c_4^0, c_2^2 = c_3, c_2^0 = c_4, c_3^0 = c_4^2,$$

whence $c_1 = c_4 = 1, c_3 = c_2^2 > 0$;

– for $e_1 = 1$, $e_2 = 2, e_3 = 3$, $S = \{1\}$ $E = \{2\}$, $O = \{3\}$. Suppose $c_2 = 6$, so both the primes 2 and 3 divide c_2. From $c_1 = c_2^0$, $c_1^2 = c_3^0$, $c_2^2 = c_3$ we get $c_1 = 1$ and $c_3 = 36$. We notice that $2 \mid c_3$ and $3 \mid c_3$, but neither 2 nor 3 divide c_1;

– for $e_1 = e_4 = 1, e_2 = 4, e_3 = 8$ we have $S = \{1, 4\}, E = \{2, 3\}, O = \emptyset$ and

$$c_1^3 = c_2^0, c_1^7 = c_3^0, c_1^0 = c_4^0, c_2^7 = c_3^3, c_2^0 = c_4^3, c_3^0 = c_4^7.$$

whence $c_1 = c_4 = 1, c_2 = \chi^3, c_3 = \chi^7, c_2c_3 > 0$, for some $\chi \in \mathbb{Z} \setminus \{0\}$.

As regards the values $|c_i|, 1 \leq i \leq n$, setting

$$\rho := \sum_{j=1}^{n}(e_j - 1) = \sum_{j\in I}(e_j - 1), \chi := \sqrt[\rho]{\prod_{j=1}^{n} |c_j|} \in \mathbb{N} \setminus \{0\},$$

we have

$$|c_j| = \chi^{e_j - 1} \text{ for each } j \in \{1, ..., n\}. \tag{1-c}$$

In fact, since if a prime p divides at least a c_j, $j \in I$, then it divides each $c_i, i \in I$, we can express each $|c_i|, i \in I$, as $|c_i| = p_1^{a_{i,1}} \cdots p_h^{a_{i,h}}$ where $p_1, \cdots, p_h$ are the prime factors of the squarefree associate $\sqrt{\chi} = p_1 \cdots p_h$ of χ.

We have

$$|c_i|^{e_j - 1} = |c_j|^{e_i - 1} \implies p^{a_i(e_j - 1)} = p^{a_j(e_i - 1)} \implies a_i(e_j - 1) = a_j(e_i - 1)$$

whence $a_i = a_j \iff e_i = e_j$ and $a_i > a_j \iff e_j < e_i$.

Thus the c_is with minimal e_i minimalize also all $a_{i,l}, 1 \leq l \leq h$.

We moreover have $a_{j,l} = \frac{a_{i,l}(e_j - 1)}{(e_i - 1)}, 1 \leq l \leq h$.

Therefore $\prod_{j=1}^{n} |c_j| = \prod_{j\in I} |c_j| = \prod_{j=1}^{n} \prod_{l=1}^{h} p_l^{a_{j,l}} = \prod_{l=1}^{h} p_l^{\frac{a_{i,l} \sum_{j=1}^{n}(e_j - 1)}{e_i - 1}} = \prod_{l=1}^{h} p_l^{\frac{a_{i,l}\rho}{e_i - 1}}$ whence

$$\chi := \sqrt[\rho]{\prod_{j=1}^{n} |c_j|} = \prod_{l=1}^{h} p_l^{\frac{a_{i,l}}{e_i - 1}} = \prod_{l=1}^{h} p_l^{\frac{a_{j,l}}{e_j - 1}}$$

and (1-c).

The formula (1-c) allows to reformulate (1-b) as

$$|c_j|^{e_i - 1} = |c_i|^{e_j - 1} = \chi^{(e_i - 1)(e_j - 1)}. \tag{1-d}$$

Note that we have

$$\begin{aligned}\chi^{(e_i^{a_i}-1)(e_j^{a_j}-1)} = \chi^{(e_i-1)\gamma(a_i,e_i)(e_j-1)\gamma(a_j,e_j)} &= |c_i|^{(e_j-1)\gamma(a_i,e_i)\gamma(a_j,e_j)} = |c_i|^{(e_j^{a_j}-1)\gamma(a_i,e_i)} \\ &= |c_j|^{(e_i-1)\gamma(a_i,e_i)\gamma(a_j,e_j)} = |c_j|^{(e_i^{a_i}-1)\gamma(a_j,e_j)}\end{aligned}$$

and

$$|c_i|^{\gamma(a_i,e_i)}|c_j|^{e_i^{a_i}\gamma(a_j,e_j)} = |c_i|^{e_j^{a_j}\gamma(a_i,e_i)}|c_j|^{\gamma(a_j,e_j)} = \chi^{e_i^{a_i}e_j^{a_j}-1}. \tag{1-e}$$

Now we explain how to deduce a general formula for the product of two "monomials" in this context.

To avoid cumbersome and useless case-to-case studies, let us simply assume $c_i > 0$ for each i; under this restricted assumption, a series of inductive arguments allows to deduce

$$Y_i * x^\alpha = c_i^\alpha x^{\alpha e_i} Y_i, \tag{2-a}$$

$$Y_j^{a_j} * x^{b_0} = c_j^{b_0\gamma(a_j,e_j)} x^{b_0 e_j^{a_j}} Y_j^{a_j}. \tag{2-b}$$

Substituing $c_j = \chi^{e_j-1}$ and $c_i = \chi^{e_i-1}$ we get

$$c_j^{b_0\gamma(a_j,e_j)} c_i^{b_0 e_j^{a_j}\gamma(a_i,e_i)} = \chi^{b_0(e_j^{a_j}e_i^{a_i}-1)}, \tag{2-c}$$

$$Y_i^{a_i}Y_j^{a_j} * x^{b_0} = c_j^{b_0\gamma(a_j,e_j)} c_i^{b_0 e_j^{a_j}\gamma(a_i,e_i)} x^{b_0 e_j^{a_j}e_i^{a_i}} Y_i^{a_i}Y_j^{a_j} = \chi^{b_0(e_j^{a_j}e_i^{a_i}-1)} x^{b_0 e_j^{a_j}e_i^{a_i}} Y_i^{a_i}Y_j^{a_j}. \tag{2-d}$$

In conclusion

$$(ax^{a_0}Y_1^{a_1}\cdots Y_n^{a_n}) * (bx^{b_0}Y_1^{b_1}\cdots Y_n^{b_n}) = ab\chi^{b_0((\prod_{i=1}^n e_i^{a_i})-1)} x^{a_0+b_0\prod_{i=1}^n e_i^{a_i}} Y_1^{a_1+b_1}\cdots Y_n^{a_n+b_n}. \tag{2-e}$$

Note that associativity is verified by

$$\begin{aligned}&\left[\left(ax^{a_0}Y_1^{a_1}\cdots Y_n^{a_n}\right) * \left(bx^{b_0}Y_1^{b_1}\cdots Y_n^{b_n}\right)\right] * \left(dx^{d_0}Y_1^{d_1}\cdots Y_n^{d_n}\right) \\ = \;& \left[ab\chi^{b_0((\prod_{i=1}^n e_i^{a_i})-1)} x^{a_0+b_0\prod_{i=1}^n e_i^{a_i}} Y_1^{a_1+b_1}\cdots Y_n^{a_n+b_n}\right] * \left(dx^{d_0}Y_1^{d_1}\cdots Y_n^{d_n}\right) \\ = \;& abd\chi^{b_0((\prod_{i=1}^n e_i^{a_i})-1)+d_0\left(\left(\prod_{i=1}^n e_i^{a_i+b_i}\right)-1\right)} x^{a_0+b_0\prod_{i=1}^n e_i^{a_i}+d_0\prod_{i=1}^n e_i^{a_i+b_i}} Y_1^{a_1+b_1+d_1}\cdots Y_n^{a_n+b_n+d_n}\end{aligned}$$

and

$$\begin{aligned}&\left(ax^{a_0}Y_1^{a_1}\cdots Y_n^{a_n}\right) * \left[\left(bx^{b_0}Y_1^{b_1}\cdots Y_n^{b_n}\right) * \left(dx^{d_0}Y_1^{d_1}\cdots Y_n^{d_n}\right)\right] \\ = \;& \left(ax^{a_0}Y_1^{a_1}\cdots Y_n^{a_n}\right) * \left[bd\chi^{d_0\left(\left(\prod_{i=1}^n e_i^{b_i}\right)-1\right)} x^{b_0+d_0\prod_{i=1}^n e_i^{b_i}} Y_1^{b_1+d_1}\cdots Y_n^{b_n+d_n}\right] \\ = \;& abd\chi^{d_0\left(\left(\prod_{i=1}^n e_i^{b_i}\right)-1\right)+\left(b_0+d_0\left(\prod_{i=1}^n e_i^{b_i}\right)\right)\left(\left(\prod_{i=1}^n e_i^{a_i}\right)-1\right)} x^{a_0+\left(b_0+d_0\prod_{i=1}^n e_i^{b_i}\right)\prod_{i=1}^n e_i^{a_i}} \prod_{i=1}^n Y_i^{a_i+b_i+d_i} \\ = \;& abd\chi^{b_0((\prod_{i=1}^n e_i^{a_i})-1)+d_0\left(\left(\prod_{i=1}^n e_i^{a_i+b_i}\right)-1\right)} x^{a_0+b_0\prod_{i=1}^n e_i^{a_i}+d_0\prod_{i=1}^n e_i^{a_i+b_i}} Y_1^{a_1+b_1+d_1}\cdots Y_n^{a_n+b_n+d_n}.\end{aligned}$$

□

2 Buchberger Theory

In this section, R is a not necessarily commutative domain and R a multivariate Ore extension.

2.1 Term ordering

For each $m \in \mathbb{N}$, the free R-module R^m – the canonical basis of which will be denoted $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ – is an (R, R)-bimodule with basis the set of the *terms*

$$\mathcal{T}^{(m)} := \{t\mathbf{e}_i : t \in \mathcal{T}, 1 \leq i \leq m\}.$$

If we impose on $\mathcal{T}^{(m)}$ a total ordering $<$, then each $f \in \mathsf{R}^m$ has a unique representation as an ordered linear combination of terms $t \in \mathcal{T}^{(m)}$ with coefficients in R:

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in R \setminus \{0\}, t_i \in \mathcal{T}^{(m)}, t_1 > \cdots > t_s.$$

The *support* of f is the set $\mathrm{supp}(f) := \{t \,|\, c(f, t) \neq 0\}$.

W.r.t. $<$ we denote $\mathbf{T}(f) := t_1$ the *maximal term* of f, $\mathrm{lc}(f) := c(f, t_1)$ its *leading coefficient* and $\mathbf{M}(f) := c(f, t_1)t_1$ its *maximal monomial*.

If we denote, following [45, 46], $\mathsf{M}(\mathsf{R}^m) := \{ct\mathbf{e}_i \,|\, c \in R \setminus \{0\}, t \in \mathcal{T}, 1 \leq i \leq m\}$, for each $f \in \mathsf{R}^m \setminus \{0\}$, the unique finite representation above can be reformulated

$$f = \sum_{\tau \in \mathrm{supp}(f)} m_\tau,\ m_\tau = c(f, \tau)\tau,$$

as a sum of elements of the *monomial set* $\mathsf{M}(\mathsf{R}^m)$.

Fixed a term ordering $\prec$ on $\mathcal{T}$ a $\prec$-compatible term ordering $<$ on $\mathcal{T}^{(m)}$ is a well-ordering on $\mathcal{T}^{(m)}$ which satisfies

$$\omega_1 \prec \omega_2 \implies \omega_1 t < \omega_2 t,\ t\omega_1 < t\omega_2 \text{ for each } t \in \mathcal{T}^{(m)},\ \omega_1, \omega_2 \in \mathcal{T}.$$

From now on, we suppose $<$ compatible with a given term ordering $\prec$ on $\mathcal{T}$.

While a multivariate Ore extension does not satisfy commutativity between terms and coefficients,

$$t \star r = rt \text{ for each } r \in R \setminus \{0\}, t \in \mathcal{T}^{(m)},$$

it however satisfies

$$\mathbf{M}(t \star r) = \alpha_t(r)t, \text{ for each } r \in R \setminus \{0\}, t \in \mathcal{T}^{(m)}; \tag{3}$$

moreover, while R is not a monoid ring under the multiplication $\star$, so that in particular we cannot claim $\tau \star \omega \in \mathcal{T}$ for $\tau, \omega \in \mathcal{T}$, however $\tau \star \omega$ satisfies

$$\mathbf{T}(\tau \star \omega) = \tau \circ \omega \tag{4}$$

where we have denoted $\circ$ the (commutative) multiplication of $\mathcal{T}$; similarly, for $n \in \mathsf{M}(\mathsf{R}^m)$ and $m_l, m_r \in \mathsf{M}(\mathsf{R}) = \{ct : c \in R \setminus \{0\}, t \in \mathcal{T}\}$ we have $\mathsf{M}(m_l \star n \star m_r) = m_l * n * m_r$.

In conclusion

Corollary 15. *If $<$ is a term ordering on $\mathcal{T}$ and $<$ is a $\prec$-compatible term ordering on $\mathcal{T}^{(m)}$, then, for each $l, r \in \mathsf{R}$ and $f \in \mathsf{R}^{(m)}$,*

1. $\mathbf{M}(l \star f) = \mathbf{M}(\mathbf{M}(l) \star \mathbf{M}(f)) = \mathbf{M}(l) * \mathbf{M}(f)$*;*
2. $\mathbf{M}(f \star r) = \mathbf{M}(\mathbf{M}(f) \star \mathbf{M}(r)) = \mathbf{M}(f) * \mathbf{M}(r)$*;*
3. $\mathbf{M}(l \star f \star r) = \mathbf{M}(\mathbf{M}(l) \star \mathbf{M}(f) \star \mathbf{M}(r)) = \mathbf{M}(l) * \mathbf{M}(f) * \mathbf{M}(r)$.
4. $\mathbf{T}(l \star f) = \mathbf{T}(l) \circ \mathbf{T}(f)$*;*
5. $\mathbf{T}(f \star r) = \mathbf{T}(f) \circ \mathbf{T}(r)$*;*
6. $\mathbf{T}(l \star f \star r) = \mathbf{T}(l) \circ \mathbf{T}(f) \circ \mathbf{T}(r)$.

2.2 Gröbner Bases

Consider a term ordering on $\mathcal{T}^{(m)}$, compatible with a term ordering on $\mathcal{T}$; with a slight abuse of notation we denote both of them by $<$.

For any set $F \subset \mathsf{R}^m$, we call $\mathbb{I}_L(F), \mathbb{I}_R(F), \mathbb{I}_2(F)$ the left (resp. right, bilateral) module generated by F, and

- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\} \subset \mathcal{T}^{(m)}$;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$.
- $\mathbf{T}_L(F) := \{\mathbf{T}(\lambda \star f) : \lambda \in \mathcal{T}, f \in F\} = \{\lambda \circ \mathbf{T}(f) : \lambda \in \mathcal{T}, f \in F\} \subset \mathcal{T}^{(m)}$;
- $\mathbf{M}_L(F) := \{\mathbf{M}(a\lambda \star f) : a \in R \setminus \{0\},\ \lambda \in \mathcal{T}, f \in F\} = \{m * \mathbf{M}(f) : m \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$;
- $\mathbf{T}_R(F) := \{\mathbf{T}(f \star \rho) : \rho \in \mathcal{T}, f \in F\} = \{\mathbf{T}(f) \circ \rho : \rho \in \mathcal{T}, f \in F\} \subset \mathcal{T}^{(m)}$;
- $\mathbf{M}_R(F) := \{\mathbf{M}(f \star b\rho) : b \in R \setminus \{0\},\ \rho \in \mathcal{T}, f \in F\} = \{\mathbf{M}(f) * n : n \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$;
- $\mathbf{T}_2(F) := \{\mathbf{T}(\lambda \star f \star \rho) : \lambda, \rho \in \mathcal{T}, f \in F\} = \{\lambda \circ \mathbf{T}(f) \circ \rho : \lambda, \rho \in \mathcal{T}, f \in F\} \subset \mathcal{T}^{(m)}$;
- $\mathbf{M}_2(F) := \{\mathbf{M}(a\lambda \star f \star b\rho) : a, b \in R \setminus \{0\}, \lambda, \rho \in \mathcal{T}, f \in F\} = \{m * \mathbf{M}(f) * n : m, n \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$.

Following an intutition by Weispfenning [53] we further denote

- $\mathbb{I}_W(F)$ the *restricted* module generated by F,

$$\mathbb{I}_W(F) := \mathrm{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{T}, f \in F),$$

- $\mathbf{T}_W(F) := \mathbf{T}_R(F)$,
- $\mathbf{M}_W(F) := \{\mathbf{M}(af \star \rho) : a \in R \setminus \{0\}, \rho \in \mathcal{T}, f \in F\} = \{a\mathbf{M}(f) * \rho : a \in R \setminus \{0\}, \rho \in \mathcal{T}, f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$.

If R is a skew field, for each set $F \subset \mathsf{R}^m$ we have

$$\begin{array}{rcccl} \mathbf{M}_L(F) & = & \mathbf{M}\{\mathbb{I}_L(\mathbf{M}\{F\})\} & = & \mathbb{I}_L(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m), \\ \mathbf{M}_R(F) & = & \mathbf{M}\{\mathbb{I}_R(\mathbf{M}\{F\})\} & = & \mathbb{I}_R(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m), \\ \mathbf{M}_2(F) & = & \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\} & = & \mathbb{I}_2(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m), \\ \mathbf{M}_W(F) & = & \mathbf{M}\{\mathbb{I}_W(\mathbf{M}\{F\})\} & = & \mathbb{I}_W(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m). \end{array} \tag{5}$$

Notation 16. From now on, in order to avoid cumbersome notation and boring repetitions, we will drop the subscripts when it will be clear of which kind of module (left, right, bilateral, restricted) we are discussing. As a consequence, the four statements of (5) will be summarized as

$$\mathbf{M}(F) = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m).$$

Similarly, we formulate a (left, right, bilateral, restricted) definition simply either for the left or for the bilateral case leaving to the reader the task to convert to the other cases.

For instance condition (ii) below is stated for the bilateral case; it would be reformulated:

left case for each $f \in \mathbb{I}(F)$ there are $g \in F, a \in R\backslash\{0\}, \lambda \in \mathcal{T}$ such that $\mathbf{M}(f) = a\lambda * \mathbf{M}(g) = \mathbf{M}(a\lambda \star g)$,

right case for each $f \in \mathbb{I}(F)$ there are $g \in F, b \in R\backslash\{0\}, \rho \in \mathcal{T}$ such that $\mathbf{M}(f) = \mathbf{M}(g) * b\rho = \mathbf{M}(g \star b\rho)$,

restricted case for each $f \in \mathbb{I}(F)$ there are $g \in F, a \in R\backslash\{0\}, \rho \in \mathcal{T}$ such that $\mathbf{M}(f) = a\mathbf{M}(g) * \rho = \mathbf{M}(ag \star \rho)$,

□

The conditions in (5) imply that, if R is a skew field, the following conditions are equivalent and can be naturally chosen as definition of Gröbner bases:

1. $\mathbf{M}(\mathbb{I}(F)) = \mathbf{M}\{\mathbb{I}(F)\} = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$,
2. for each $f \in \mathbb{I}(F)$ there is $g \in F$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$.

But in general between these statements there is just the implication (2) $\implies$ (1).

Thus [40], there are two alternative natural definitions for the concept of Gröbner bases:

– a stronger one which satisfies the following equivalent conditions:

  (i). for each $f \in \mathbb{I}(F)$ there is $g \in F$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$,

  (ii). for each $f \in \mathbb{I}(F)$ there are $g \in F$, $a, b \in R \setminus \{0\}, \lambda, \rho \in \mathcal{T}$ such that $\mathbf{M}(f) = a\lambda * \mathbf{M}(g) * b\rho = \mathbf{M}(a\lambda \star g \star b\rho)$,

  (iii). $\mathbf{M}(\mathbb{I}(F)) = \mathbf{M}\{\mathbb{I}(F)\} = \mathbf{M}(F)$;

– and a weaker one which satisfies the following equivalent conditions:

(iv). for each $f \in \mathbb{I}(F)$ there are $g_i \in F$, $a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}$ for which, denoting $\tau_i := \mathbf{T}(g_i)$, one has

- $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$ for each i, and $\mathrm{lc}(f) = \sum_i a_i \alpha_{\lambda_i}(\mathrm{lc}(g_i))\alpha_{\lambda_i\tau_i}(b_i)$
- $\mathbf{M}(f) = \sum_i a_i\lambda_i * \mathbf{M}(g_i) * b_i\rho_i = \sum_i \mathbf{M}(a_i\lambda_i \star g_i \star b_i\rho_i)$;

(v). $\mathbf{M}(\mathbb{I}(F)) = \mathbf{M}\{\mathbb{I}(F)\} = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$;

if moreover R is a skew field $\mathbf{M}(F) = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\}$ so that conditions (i-v) above are all equivalent and are also equivalent to

(vi). $\mathbf{T}(f) = \lambda \circ \mathbf{T}(g) \circ \rho$ for some $g \in F$, $\lambda, \rho \in \mathcal{T}$.

Example 17. Let us now specialize the ring of Example 14 to the case

$$n = 3, e_1 = 2, e_2 = 3, e_3 = 4, \chi = 5, c_1 = 5, c_2 = 5^2, c_3 = 5^3$$

and remark that

$$ax^{a_0}Y_1^{a_1}Y_2^{a_2}Y_3^{a_3} * bx^{b_0}Y_1^{b_1}Y_2^{b_2}Y_3^{b_3} = ab5^{b_0(2^{a_1}3^{a_2}4^{a_3}-1)}x^{a_0+b_0 2^{a_1}3^{a_2}4^{a_3}}Y_1^{a_1+b_1}Y_2^{a_2+b_2}Y_3^{a_3+b_3}.$$

As a consequence, for each $(b_0, b_1, b_2, b_3), (j_0, j_1, j_2, j_3) \in \mathbb{N}^4$, $b, j \in \mathbb{Z}$

$$jx^{j_0}Y_1^{j_1}Y_2^{j_2}Y_3^{j_3} \in \mathbb{I}_L(bx^{b_0}Y_1^{b_1}Y_2^{b_2}Y_3^{b_3})$$

if and only if

$$a_1 := j_1 - b_1 \geq 0, a_2 := j_2 - b_2 \geq 0, a_3 := j_3 - b_3 \geq 0, a_0 := j_0 - b_0 2^{a_1}3^{a_2}4^{a_3} \geq 0 \quad (6)$$

and $b5^{b_0(2^{a_1}3^{a_2}4^{a_3}-1)} \mid j$.

Note that if we set $y := 5x$ then for each $(b_1, b_2, b_3), (j_1, j_2, j_3) \in \mathbb{N}^3$ and $b(y), j(y) \in \mathbb{Z}[y] \subset R$

$$j(y)Y_1^{j_1}Y_2^{j_2}Y_3^{j_3} \in \mathbb{I}_L(b(y)Y_1^{b_1}Y_2^{b_2}Y_3^{b_3})$$

if and only if, not only (6) but also $\boxed{b(y^{2^{a_1}3^{a_2}4^{a_3}}) \mid j(y).}$

Definition 18. Let $\mathsf{I} \subset \mathsf{R}^m$ be a (left, right, bilateral, restricted) module and $G \subset \mathsf{I}$.

- G will be called
  - a (left, right, bilateral, restricted) *weak Gröbner basis* (*Gröbner basis* for short) of I if

$$\mathbf{M}\{\mathsf{I}\} = \mathbf{M}(\mathsf{I}) = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{G\})\} = \mathbb{I}(\mathbf{M}\{G\}) \cap \mathsf{M}(\mathsf{R}^m),$$

    id est if G satisfies conditions (iv-v) w.r.t. the module $\mathsf{I} = \mathbb{I}(G)$; in particular $\mathbf{M}\{G\}$ generates the (left, right, bilateral, restricted) module $\mathbf{M}(\mathsf{I}) \subset \mathsf{R}^m$;
  - a (left, right, bilateral, restricted) *strong Gröbner basis* of I if for each $f \in \mathsf{I}$ there is $g \in G$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$, *id est* if G satisfies conditions (i-iii) w.r.t. the module $\mathsf{I} = \mathbb{I}(G)$.

– We say that $f \in \mathsf{R}^m \setminus \{0\}$ has

  – a left *Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{u} l_i \star g_i$, with $l_i \in \mathsf{R}, g_i \in G$ and $\mathbf{T}(l_i) \circ \mathbf{T}(g_i) \leq \mathbf{T}(f)$ for each i;
  – a left *(weak) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i \lambda_i \star g_i$, with $a_i \in R \setminus \{0\}, \lambda_i \in \mathcal{T}, g_i \in G$ and $\lambda_i \circ \mathbf{T}(g_i) \leq \mathbf{T}(f)$ for each i;
  – a left *(strong) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i \lambda_i \star g_i$, with $a_i \in R \setminus \{0\}, \lambda_i \in \mathcal{T}, g_i \in G$ and

$$\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(g_1) > \lambda_i \circ \mathbf{T}(g_i) \text{ for each } i;$$

  – a right *Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{u} g_i \star r_i$, with $r_i \in \mathsf{R}, g_i \in G$ and $\mathbf{T}(g_i) \circ \mathbf{T}(r_i) \leq \mathbf{T}(f)$ for each i;
  – a right *(weak) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} g_i \star b_i \rho_i$, with $b_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_i \in G$ and $\mathbf{T}(g_i) \circ \rho_i \leq \mathbf{T}(f)$ for each i;
  – a right *(strong) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} g_i \star b_i \rho_i$, with $b_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_i \in G$ and

$$\mathbf{T}(f) = \mathbf{T}(g_1) \circ \rho_1 > \mathbf{T}(g_i) \circ \rho_i \text{ for each } i;$$

  – a bilateral *(weak) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i \lambda_i \star g_i \star b_i \rho_i$, with $a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, g_i \in G$ and $\lambda_i \circ \mathbf{T}(g_i) \circ \rho_i \leq \mathbf{T}(f)$ for each i;
  – a bilateral *(strong) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i \lambda_i \star g_i \star b_i \rho_i$, with $a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, g_i \in G$ and $\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(g_1) \circ \rho_1 > \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$ for each i.
  – a restricted *(weak) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i g_i \star \rho_i$, with $a_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_i \in G$ and $\mathbf{T}(g_i) \circ \rho_i \leq \mathbf{T}(f)$ for each i;
  – a restricted *(strong) Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^{\mu} a_i g_i \star \rho_i$, with $a_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_i \in G$ and $\mathbf{T}(f) = \mathbf{T}(g_1) \circ \rho_1 > \mathbf{T}(g_i) \circ \rho_i$ for each i.

– For $f \in \mathsf{R}^m \setminus \{0\}, F \subset \mathsf{R}^m$, an element $h := \mathrm{NF}(f, F) \in \mathsf{R}^m$ is called a

  – (left, right, bilateral, restricted) *(weak) normal form* of f w.r.t. F, if

    $f - h \in \mathbb{I}(F)$ has a weak Gröbner representation in terms of F, and
    $h \neq 0 \implies \mathbf{M}(h) \notin \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\}$;
  – (left, right, bilateral, restricted) *strong normal form* of f w.r.t. F, if

    $f - h \in \mathbb{I}(F)$ has a strong Gröbner representation in terms of F, and
    $h \neq 0 \implies \mathbf{M}(h) \notin \mathbf{M}(F)$. □

Proposition 19. *(*cf. *[45, 46]) For any set $F \subset \mathsf{R}^m \setminus \{0\}$, among the following conditions:*

1. *$f \in \mathbb{I}(F) \iff$ it has a (left, right, bilateral, restricted) strong Gröbner representation $f = \sum_{i=1}^{\mu} a_i\lambda_i \star g_i \star b_i\rho_i$ in terms of F which further satisfies*

$$\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(g_1) \circ \rho_1 > \cdots > \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i > \cdots ;$$

2. *$f \in \mathbb{I}(F) \iff$ it has a (left, right, bilateral, restricted) strong Gröbner representation in terms of F;*

3. *F is a (left, right, bilateral, restricted) strong Gröbner basis of $\mathbb{I}(F)$;*

4. *$f \in \mathbb{I}(F) \iff$ it has a (left, right, bilateral, restricted) weak Gröbner representation in terms of F;*

5. *F is a (left, right, bilateral, restricted) Gröbner basis of $\mathbb{I}(F)$;*

6. *$f \in \mathbb{I}(F) \iff$ it has a (left, right) Gröbner representation in terms of F;*

7. *for each $f \in \mathsf{R}^m \setminus \{0\}$ and any (left, right, bilateral, restricted) strong normal form h of f w.r.t. F we have $f \in \mathbb{I}(F) \iff h = 0$;*

8. *for each $f \in \mathsf{R}^m \setminus \{0\}$ and any (left, right, bilateral, restricted) weak normal form h of f w.r.t. F we have $f \in \mathbb{I}(F) \iff h = 0$;*

there are the implications

$$\begin{array}{ccccccc} (1) & \Leftrightarrow & (2) & \Rightarrow & (4) & \Leftrightarrow & (6) \\ & \nearrow & \Updownarrow & & \Updownarrow & \nwarrow & \\ (7) & \Leftarrow & (3) & \Rightarrow & (5) & \Rightarrow & (8) \end{array}$$

If R is a skew field we have also the implication (4) $\implies$ (2) *and as a consequence also* (5) $\implies$ (3)*.*

Proof. The implications (1) $\implies$ (2) $\implies$ (4) $\iff$ (6), (3) $\implies$ (5), (2) $\implies$ (3) and (4) $\implies$ (5) are trivial.

(3) $\implies$ (1): for each $f \in \mathbb{I}_2(F)$, by assumption, there are elements $g \in F, m = a\lambda, n = b\rho \in \mathsf{M}(\mathsf{R})$ such that $\mathbf{M}(f) = \mathbf{M}(m \star g \star n)$. Thus $\mathbf{T}(f) = \mathbf{T}(m \star g \star n) = \lambda \circ \mathbf{T}(g) \circ \rho$ and, denoting $f_1 := f - m \star g \star n$, we have $\mathbf{T}(f_1) < \mathbf{T}(f)$ so the claim follows by induction, since $<$ is a well ordering.

(5) $\implies$ (4): similarly, for each $f \in \mathbb{I}_2(F)$ by assumption there are elements $g_i \in F, \mathbf{T}(g_i) := \tau_i \mathbf{e}_{l_i}, m_i = a_i\lambda_i, n_i = b_i\rho_i \in \mathsf{M}(\mathsf{R})$ such that

- $\mathbf{T}(f) = \mathbf{T}(\lambda_i \star g_i \star \rho_i) = \lambda_i \circ \tau_i \circ \rho_i \mathbf{e}_{l_i}$ for each i,
- $\mathrm{lc}(f) = \sum_i a_i \alpha_{\lambda_i}(\mathrm{lc}(g_i))\alpha_{\lambda_i\tau_i}(b_i)$.

It is then sufficient to denote $f_1 := f - \sum_i m_i \star g_i \star n_i$ in order to deduce the claim by induction, since $\mathbf{T}(f_1) < \mathbf{T}(f)$ and $<$ is a well ordering.

(4) $\implies$ (2): let $f \in \mathbb{I}_2(F) \setminus \{0\}$; (4) implies the existence of $g \in F, \lambda, \rho \in \mathcal{T}$, such that $\mathbf{T}(f) = \lambda \circ \mathbf{T}(g) \circ \rho$. Then setting $f_1 := f - \mathrm{lc}(f)\Big(\alpha_\lambda\left(\mathrm{lc}(g)\right)\Big)^{-1} \lambda \star g \star \rho$ we deduce the claim by induction, since $\mathbf{T}(f_1) < \mathbf{T}(f)$ and $<$ is a well ordering.

(3) $\implies$ (7) and (5) $\implies$ (8): either

- $h = 0$ and $f = f - h \in \mathbb{I}(F)$ or
- $h \neq 0$, $\mathbf{M}(h) \notin \mathbf{M}(\mathbb{I}(F))$, $h \notin \mathbb{I}(F)$ and $f \notin \mathbb{I}(F)$.

(7) $\implies$ (2) and (8) $\implies$ (4): for each $f \in \mathbb{I}(F)$, its normal form is $h = 0$ and $f = f - h$ has a strong (resp.: weak) Gröbner representation in terms of F.

□

Proposition 20. *(Compare [31, Proposition 22.2.10]) If F is a (weak, strong) Gröbner basis of $\mathsf{I} := \mathbb{I}(F)$, then the following holds:*

1. *Let $g \in \mathsf{R}^m$ be a (weak, strong) normal form of f w.r.t. F. If $g \neq 0$, then*

$$\mathbf{T}(g) = \min\{\mathbf{T}(h) : h - f \in \mathbb{I}(F)\}.$$

2. *Let $f, f' \in \mathsf{R}^m \setminus \mathsf{I}$ be such that $f - f' \in \mathsf{I}$. Let g be a (weak, strong) normal form of f w.r.t. F and g' be a (weak, strong) normal form of f' w.r.t. F. Then*
   - $\mathbf{T}(g) = \mathbf{T}(g') =: \tau$ *and*
   - $\mathrm{lc}(g) - \mathrm{lc}(g') \in \mathsf{I}_\tau := \{\mathrm{lc}(f) : f \in \mathsf{I}, \mathbf{T}(f) = \tau\} \cup \{0\} \subset R$.

Proof.

1. Let $h \in \mathsf{R}^m$ be such that $h - f \in \mathsf{I}$; then $h - g \in \mathsf{I}$ and $\mathbf{M}(h - g) \in \mathbf{M}\{\mathsf{I}\}$. If $\mathbf{T}(g) > \mathbf{T}(h)$ then $\mathbf{M}(h - g) = \mathbf{M}(g) \notin \mathbf{M}\{\mathsf{I}\}$, giving a contradiction.

2. The assumption implies that $f - g' \in \mathsf{I}$ so that, by the previous result, $\mathbf{T}(g) \leq \mathbf{T}(g')$. Symmetrically, $f' - g \in \mathsf{I}$ and $\mathbf{T}(g') \leq \mathbf{T}(g)$. Therefore $\mathbf{T}(g) = \mathbf{T}(g') = \tau$; moreover, either
   - $\mathbf{T}(g - g') < \tau$ and $\mathbf{M}(g) = \mathbf{M}(g')$ so that $\mathrm{lc}(g) = \mathrm{lc}(g')$ or
   - $\mathbf{T}(g - g') = \tau$ and $\mathbf{M}(g - g') = \mathbf{M}(g) - \mathbf{M}(g') = \Big(\mathrm{lc}(g) - \mathrm{lc}(g')\Big)\tau$; thus, since $g - g' \in \mathsf{I}$, $\mathrm{lc}(g) - \mathrm{lc}(g') \in \mathsf{I}_\tau$.

□

2.3 Canonical forms (skew field case)

If $R := \mathbb{K}$ is a skew field, for any set $F \subset \mathsf{R}^m$ we denote $\mathbf{N}(F)$ the (left, right, bilateral, restricted) order module $\mathbf{N}(F) := \mathcal{T}^{(m)} \setminus \mathbf{T}(F)$ and $\mathbb{K}[\mathbf{N}(F)]$ the (left, right, bilateral, restricted) $\mathbb{K}$-module $\mathbb{K}[\mathbf{N}(F)] := \mathrm{Span}_{\mathbb{K}}(\mathbf{N}(F))$.

Figure 1: Canonical Form Algorithms

$(g, \sum_{i=1}^{\mu} c_i \lambda_i \star g_i) :=$ **LeftCanonicalForm**(f, G)

where

G is the left Gröbner basis of the left module $\mathsf{I} \subset \mathsf{R}^m$,

$f \in \mathsf{R}^m$, $g \in \mathbb{K}[\mathbf{N}(\mathsf{I})]$, $c_i \in \mathbb{K} \setminus \{0\}$, $\lambda_i \in \mathcal{T}$, $g_i \in G$,

$f - g = \sum_{i=1}^{\mu} c_i \lambda_i \star g_i$ is a left strong Gröbner representation in terms of G,

$\mathbf{T}(f-g) = \lambda_1 \circ \mathbf{T}(g_1) > \lambda_2 \circ \mathbf{T}(g_2) > \cdots > \lambda_\mu \circ \mathbf{T}(g_\mu)$.

$h := f, i := 0, g := 0,$

While $h \neq 0$ **do**

$\%\%\ f = g + \sum_{j=1}^{i} c_j \lambda_j \star g_j + h,$

$\%\%\ \mathbf{T}(f-g) \geq \mathbf{T}(h);$

$\%\%\ i > 0 \implies \mathbf{T}(f-g) = \lambda_1 \circ \mathbf{T}(g_1) > \lambda_2 \circ \mathbf{T}(g_2) > \cdots > \lambda_i \circ \mathbf{T}(g_i) > \mathbf{T}(h);$

If $\mathbf{T}(h) \in \mathbf{T}_L(G)$ **do**

Let $\lambda \in \mathcal{T}, \gamma \in G : \lambda \circ \mathbf{T}(\gamma) = \mathbf{T}(h)$

$\bullet\ i := i+1, c_i := \mathrm{lc}(h)\alpha_\lambda \left(\mathrm{lc}(\gamma)\right)^{-1}, \lambda_i := \lambda, g_i := \gamma, h := h - c_i \lambda_i g_i.$

Else

$\%\%\ \mathbf{T}(h) \in \mathbf{N}(\mathsf{I})$

$g := g + \mathbf{M}(h),\ h := h - \mathbf{M}(h)$

Definition 21. For any (left, right, bilateral, restricted) module $\mathsf{I} \subset \mathsf{R}^m$, the order module $\mathbf{N}(\mathsf{I}) := \mathcal{T}^{(m)} \setminus \mathbf{T}\{\mathsf{I}\}$ is called the *escalier* of I.

We easily obtain the notion, the properties and the computational algorithm (Figure 1 and Remark 25) of (left, right, bilateral, restricted) canonical forms:

Lemma 22. (cf. [31, Lemma 22.2.12]) *Let $\mathsf{I} \subset \mathsf{R}^m$ be a (left, right, bilateral, restricted) module. If $R = \mathbb{K}$ is a skew field and denoting A the (left, right, bilateral, restricted) module $\mathsf{A} := \mathsf{R}^m/\mathsf{I}$ it holds*

1. $\mathsf{R}^m \cong \mathsf{I} \oplus \mathbb{K}[\mathbf{N}(\mathsf{I})]$;
2. $\mathsf{A} \cong \mathbb{K}[\mathbf{N}(\mathsf{I})]$;
3. *for each $f \in \mathsf{R}^m$, there is a unique*

$$g := \mathrm{Can}(f, \mathsf{I}) = \sum_{t \in \mathbf{N}(\mathsf{I})} \gamma(f, t, <)t \in \mathbb{K}[\mathbf{N}(\mathsf{I})]$$

   such that $f - g \in \mathsf{I}$.

   Moreover:

   (a) $\mathrm{Can}(f_1, \mathsf{I}) = \mathrm{Can}(f_2, \mathsf{I}) \iff f_1 - f_2 \in \mathsf{I}$;

   (b) $\mathrm{Can}(f, \mathsf{I}) = 0 \iff f \in \mathsf{I}$.

4. *For each $f \in \mathsf{R}^m$, $f - \mathrm{Can}(f, \mathsf{I})$ has a (left, right, bilateral, restricted) strong Gröbner representation in terms of any Gröbner basis.*

Definition 23. (cf. [31, Definition 22.2.13]) For each $f \in \mathsf{R}^m$ the unique element

$$g := \mathrm{Can}(f, \mathsf{I}) \in \mathbb{K}[\mathbf{N}(\mathsf{I})]$$

such that $f - g \in \mathsf{I}$ will be called the (left, right, bilateral, restricted) *canonical form* of f w.r.t. I. □

Corollary 24. (cf. [31, Corollary 22.3.14]) *If $R = \mathbb{K}$ is a skew field, there is a unique set $G \subset \mathsf{I}$ such that*

- $\mathbf{T}\{G\}$ *is an irredundant basis of* $\mathbf{T}(\mathsf{I})$*;*
- *for each $g \in G, \mathrm{lc}(g) = 1$;*
- *for each $g \in G, g = \mathbf{T}(g) - \mathrm{Can}(\mathbf{T}(g), \mathsf{I})$.*

G is called the (left, right, bilateral, restricted) reduced Gröbner basis *of* I. □

Remark 25. As regards Figure 1, we remark that the corresponding algorithm in the right, bilateral and restricted cases can be obtained from the one stated above via trivial modifications. The only nontrivial part is the one marked with • in the algorithm, which respectively becomes:

- **Left:** $i := i + 1, c_i := \mathrm{lc}(h)\alpha_\lambda\,(\mathrm{lc}(\gamma))^{-1}\,, \lambda_i := \lambda, g_i := \gamma, h := h - c_i\lambda_i g_i$;

- **Right:** $i := i+1, d_i := \alpha^{-1}_{\mathbf{T}(\gamma)}\left(\mathrm{lc}(h)\,\mathrm{lc}(\gamma)^{-1}\right), \rho_i := \rho, g_i := \gamma, h := h - g_i \star d_i\rho_i$;
- **Bilateral:** $i := i+1, c_i := \mathrm{lc}(h)\alpha_\lambda\left(\mathrm{lc}(\gamma)\right)^{-1}, \lambda_i := \lambda, \rho_i := \rho, g_i := \gamma, h := h - c_i\lambda_i \star g_i \star \rho_i$;
- **Restricted:** $i := i+1, c_i := \mathrm{lc}(h)\,\mathrm{lc}(\gamma)^{-1}, \rho_i := \rho, g_i := \gamma, h := h - c_i g_i \star \rho_i$.

Note that the algorithm described for right canonical forms is assuming that each α_i is an automorphism; alternatively we can assume that R is given as a right R-module in which case the theory can be developed symmetrically.

3 Szekeres Theory

In this section, R is a non necessarily commutative domain and R a multivariate Ore extension.

Let $\mathsf{I} \subset \mathsf{R}^m$ be a (left, bilateral) module; if we denote for each $\tau \in \mathcal{T}^{(m)}$, I_τ the additive group

$$\mathsf{I}_\tau := \{\mathrm{lc}(f) : f \in \mathsf{I}, \mathbf{T}(f) = \tau\} \cup \{0\} \subset R,$$

$\mathfrak{I} := \{\mathsf{I}_\tau : \tau \in \mathcal{T}^{(m)}\}$ and, for each ideal $\mathfrak{a} \subset R$, $T_\mathfrak{a}$ and $L_\mathfrak{a}$ the sets

$$T_\mathfrak{a} := \{\tau \in \mathcal{T}^{(m)} : \mathsf{I}_\tau \supseteq \mathfrak{a}\} \subset \mathcal{T}^{(m)} \text{ and } L_\mathfrak{a} := \{\tau \in \mathcal{T}^{(m)} : \mathsf{I}_\tau = \mathfrak{a}\} \subset \mathcal{T}^{(m)},$$

we have

1. for each $\tau \in \mathcal{T}^{(m)}$, $\mathsf{I}_\tau \subset R$ is a left ideal;
2. for each ideals $\mathfrak{a}, \mathfrak{b} \subset R$, $\mathfrak{a} \subset \mathfrak{b} \implies T_\mathfrak{a} \supset T_\mathfrak{b}$;
3. $T_\mathfrak{a} = \bigsqcup_{\mathfrak{b} \supseteq \mathfrak{a}} L_\mathfrak{b}$, $L_\mathfrak{a} = T_\mathfrak{a} \setminus \bigcup_{\mathfrak{b} \supsetneq \mathfrak{a}} T_\mathfrak{b}$;
4. for terms $\tau, \omega \in \mathcal{T}^{(m)}$, $\tau \mid \omega \implies \mathsf{I}_\tau \subset \mathsf{I}_\omega$;
5. for each ideal $\mathfrak{a} \subset R$, $T_\mathfrak{a} \subset \mathcal{T}^{(m)}$ is a semigroup module. □

If R is a skew field, the situation is quite trivial: for any ideal I we have

$$\mathfrak{I} = \{(0), R\}, T_R = L_R = \mathbf{T}(\mathsf{I}), T_{(0)} = \mathcal{T}^{(m)}, L_{(0)} = \mathcal{T}^{(m)} \setminus \mathbf{T}(\mathsf{I}).$$

Szekeres notation is related with a pre-Buchberger construction of "canonical" ideals for the case of polynomial rings $R[Y_1, \ldots, Y_n]$ over a PID R.

In connection recall that [14, 15] a not necessarily commutative ring R is called a (left, right, bilateral) *Bézout ring* if every finitely generated (left, right, bilateral) ideal is principal and is called a *Bézout domain* if it is both a Bézout ring and is a domain, and remark that, if R is a noetherian (left, bilateral) Bézout ring, then for each $\tau \in \mathcal{T}^{(m)}$, there is a value $c_\tau \in R$ satisfying $\mathsf{I}_\tau = \mathbb{I}(c_\tau)$.

Definition 26. With the present notation, we call *Szekeres ideal* each ideal $\mathsf{I}_\tau \subset R$, *Szekeres level* each set $L_{\mathfrak{a}} \subset \mathcal{T}^{(m)}$ and *Szekeres semigroup* each semigroup $T_{\mathfrak{a}} \subset \mathcal{T}^{(m)}$.

Finally, if R is a noetherian left Bézout ring we call *Szekeres generator* each value $c_\tau \in R$ satisfying $\mathsf{I}_\tau = \mathbb{I}_L(c_\tau)$.

Note that if R is a noetherian Bézout ring, we have,

$$\omega \mid \tau \implies c_\tau \mid_L \alpha_\lambda(c_\omega) \text{ for each } \lambda, \rho \in \mathcal{T} \text{ s.t. } \tau = \lambda \circ \omega \circ \rho.$$

Proposition 27 (Szekeres)**.** *[51] Let R be a noetherian left Bézout ring and $\mathsf{I} \subset \mathsf{R}^m$ be a (left, bilateral) module. Denote*

$$\mathsf{T} := \left\{ \tau \in \mathcal{T}^{(m)} \text{ s.t. } c_\tau \notin \mathbb{I}(\alpha_\lambda(c_\omega),\ \omega \in \mathcal{T}^{(m)}, \lambda, \rho \in \mathcal{T}, \tau = \lambda \circ \omega \circ \rho) \right\} \subset \mathcal{T}^{(m)}$$

and fix, for each $\tau \in \mathsf{T}$, any element $f_\tau \in \mathsf{I}$ such that[2] $\mathbf{M}(f_\tau) = c_\tau \tau$.
Then the basis $S_w := \{f_\tau \text{ s.t. } \tau \in \mathsf{T}\}$ is a left/bilateral weak Gröbner basis of I.

Proof. For each $f \in \mathsf{I}$, denoting $\tau := \mathbf{T}(f)$ we have $\mathrm{lc}(f) \in \mathbb{I}_L(c_\tau)$ and $\mathrm{lc}(f) = dc_\tau$ for suitable $d \in R \setminus \{0\}$. Thus if $\tau \in \mathsf{T}$ we have $\mathbf{M}(f) = d\mathbf{M}(f_\tau)$; if, instead, $\tau \notin \mathsf{T}$ there are suitable $d_i, \in R \setminus \{0\}, \omega_i \in \mathsf{T} \subset \mathcal{T}^{(m)}, \lambda_i, \rho_i \in \mathcal{T}$ for which $\lambda_i \circ \omega_i \circ \rho_i = \tau$ and $c_\tau = \sum_i d_i \alpha_{\lambda_i}(c_{\omega_i})$ so that

$$\begin{aligned} \mathbf{M}(f) = dc_\tau \tau &= d\left(\sum_i d_i \alpha_{\lambda_i}(c_{\omega_i}) \lambda_i \circ \omega_i \circ \rho_i \right) \\ &= \sum_i (dd_i\lambda_i) \cdot (c_{\omega_i}\omega_i) \cdot \rho_i \\ &= \sum_i (dd_i\lambda_i) * \mathbf{M}(f_{\omega_i}) * \rho_i. \end{aligned}$$

□

Remark 28. Remark that in the case in which each endomorphism $\alpha_\tau, \tau \in \mathcal{T}^{(m)}$, is an automorphism, we can consider also *right* modules I to which we can associate

$$\mathsf{I}_\tau = \{\mathrm{lc}(f) : f \in \mathsf{I}, \mathbf{T}(f) = \tau\} \cup \{0\}$$

which are *right* ideals themselves; in fact if we represent $f \in \mathsf{R}^m$ as (see Remark 3) $f = \sum_{i=1}^n Y^i \bar{a}_i$ and we denote ${}_\tau\mathsf{I}$ the *right* ideal

$${}_\tau\mathsf{I} := \{c \in R : \tau c \in \mathbf{M}\{\mathsf{I}\}\} \cup \{0\} \subset R$$

then I_τ is the right ideal $\alpha_\tau({}_\tau\mathsf{I})$.

However, in this setting, Szekeres Theory can be built more easily by considering the ideals ${}_\tau\mathsf{I}$ obtained through the right representation of Remark 3 and adapting to them the results reported above.

Remark that if an endomorphism α_τ is not invertible, in general I_τ is not an ideal but just an additive group.

Finally note that for *restricted* modules, one applies *verbatim*, the classical Szekeres theory and substitute in the results above each instance of $\alpha_\lambda(c_\omega), \tau = \lambda \circ \omega \circ \rho$ with $c_\omega, \tau = \omega \circ \rho$. □

[2] Of course for the extreme case $\mathsf{I}_\tau = (0)$ so that $c_\tau = 0$, we have $f_\tau := 0$.

Example 29. In the Ore extension

$$\mathsf{R} := R[Y;\alpha], R = \mathbb{Z}_2[x] \text{ where } \alpha : R \to R : x \mapsto x^2$$

we can consider, as a left module, the two-sided ideal $\mathbb{I}_2(x) = \mathbb{I}_L\{xY^i : i \in \mathbb{N}\}$; we thus have

$$\mathsf{I}_\tau = \mathbb{I}(x) \subset R \text{ for each } \tau \in \{Y^i, i \geq 0\},$$

so that, setting $\mathfrak{a} := \mathbb{I}(x) \subset R$, it holds $\Im = \{\mathfrak{a}\}, T_\mathfrak{a} = L_\mathfrak{a} = \{Y^i : i \in \mathbb{N}\}$, and $S_w = \{xY^i : i \in \mathbb{N}\}$ is both a weak and a strong Gröbner basis of $\mathbb{I}_L(x)$.

For the right ideal $\mathbb{I}_R(xY)$ the sets I_τ are *not* ideals; we have, *e.g.*

$$\mathsf{I}_{Y^i} = \{x\phi(x^{e^i})|\phi(x) \in \mathbb{Z}_2[x]\}.$$

4 Zacharias canonical representation

Let R, R be two rings such that R is also a left R-module.
Following Zacharias approach to Buchberger Theory [54], if each module $\mathsf{I} \subset \mathsf{R}^m$ has a groebnerian property, necessarily the same property must be satisfied at least by the modules $\mathsf{I} \subset R^m \subset \mathsf{R}^m$ and thus such property in R^m can be used to devise a procedure granting the same property in R^m. The most elementary application of Zacharias approach is the generalization of the property of canonical forms from the case in which $R = \mathbb{K}$ is a skew field to the general case: all we need is an effective notion of canonical forms for modules in R:

Definition 30 (Zacharias)**.** [54] A ring R is said to have *canonical representatives* if there is an algorithm which, given an element $c \in R^m$ and a (left, bilateral, right) module $\mathsf{J} \subset R^m$, computes a *unique* element $\mathbf{Rep}(c, \mathsf{J})$ such that

- $c - \mathbf{Rep}(c, \mathsf{J}) \in \mathsf{J}$,
- $\mathbf{Rep}(c, \mathsf{J}) = 0 \iff c \in \mathsf{J}$.

The set

$$\mathbf{Rep}(\mathsf{J}) := \{\mathbf{Rep}(c, \mathsf{J}) : c \in R^m\} \cong R^m/\mathsf{J}$$

is called the *canonical Zacharias representation* of the module R^m/J. □

Remark that, for each $c, d \in R^m$ and each module $\mathsf{J} \subset R^m$, we have

$$c - d \in \mathsf{J} \iff \mathbf{Rep}(c, \mathsf{J}) = \mathbf{Rep}(d, \mathsf{J}).$$

Using Szekeres notation for a (left, right, bilateral) module $\mathsf{I} \subset \mathsf{R}^m$ we obtain

- the partition $\mathcal{T}^{(m)} = \mathbf{L}(\mathsf{I}) \sqcup \mathbf{R}(\mathsf{I}) \sqcup \mathbf{N}(\mathsf{I})$ of $\mathcal{T}^{(m)}$ where
  - $\mathbf{N}(\mathsf{I}) := \mathbf{L}_{(0)} = \{\omega \in \mathcal{T}^{(m)} : \mathsf{I}_\omega = (0)\}$,
  - $\mathbf{L}(\mathsf{I}) := \mathbf{L}_R = \{\omega \in \mathcal{T}^{(m)} : \mathsf{I}_\omega = R\}$,
  - $\mathbf{R}(\mathsf{I}) := \left\{\omega \in \mathcal{T}^{(m)} : \mathsf{I}_\omega \notin \{(0), R\}\right\}$;

– the *canonical Zacharias representation*

$$\mathbf{Rep}(\mathsf{I}) := \left\{\mathbf{Rep}(c,\mathsf{I}) : c \in \mathsf{R}^m\right\} = \bigoplus_{\mathfrak{a}\in\mathfrak{I}} \bigoplus_{\tau\in L_{\mathfrak{a}}} \mathbf{Rep}(\mathfrak{a})\tau = \bigoplus_{\tau\in\mathcal{T}^{(m)}} \mathbf{Rep}(\mathsf{I}_\tau)\tau \cong \mathsf{R}^m/\mathsf{I}$$

of the module R^m/I.

If R has canonical representatives and there is an algorithm (*cf.* Definition 40 (c), (e)) which, given an element $c \in R^m$ and a (left, right, bilateral) module $\mathsf{J} \subset R^m$ computes the unique canonical representative $\mathbf{Rep}(c,\mathsf{J})$, an easy adaptation of Figure 1 allows to extend, from the field coefficients case to the Zacharias ring [54, 32] coefficients case, the notion of canonical forms, the algorithm (Figure 2 and Remark 32) for computing them and their characterizing properties:

Lemma 31. *If R has canonical representatives, also R has canonical representatives.*

With the present notation and denoting, for a (left, right, bilateral) module $\mathsf{I} \subset \mathsf{R}^m$, A the (left, right, bilateral) module $\mathsf{A} := \mathsf{R}^m/\mathsf{I}$ it holds:

1. $\mathsf{R}^m \cong \mathsf{I} \oplus \mathbf{Rep}(\mathsf{I})$;
2. $\mathsf{A} \cong \mathbf{Rep}(\mathsf{I})$;
3. *for each $f \in \mathsf{R}^m$, there is a unique (left, right, bilateral)* canonical form *of f*

$$g := \mathrm{Can}(f,\mathsf{I}) = \sum_{\mathfrak{a}\in\mathfrak{I}} \sum_{\tau\in L_{\mathfrak{a}}} \gamma(f,\tau,\mathsf{I},<)\tau \in \mathbf{Rep}(\mathsf{I}), \quad \gamma(f,\tau,\mathsf{I},<) \in \mathbf{Rep}(\mathsf{I}_\tau),$$

such that

- $f - g \in \mathsf{I}$,
- $\gamma(f,\tau,\mathsf{I},<) = \mathbf{Rep}(\gamma(f,\tau,\mathsf{I},<),\mathsf{I}_\tau) \in \mathbf{Rep}(\mathsf{I}_\tau)$, *for each $\tau \in \mathcal{T}^{(m)}$.*

Moreover:

(a) $\mathrm{Can}(f_1,\mathsf{I}) = \mathrm{Can}(f_2,\mathsf{I}) \iff f_1 - f_2 \in \mathsf{I}$;

(b) $\mathrm{Can}(f,\mathsf{I}) = 0 \iff f \in \mathsf{I}$;

4. *for each $f \in \mathsf{R}^m$, $f - \mathrm{Can}(f,\mathsf{I})$ has a (left, right, bilateral) (weak, strong) Gröbner representation in terms of any (weak, strong) Gröbner basis.* □

Remark 32. As regards Figure 2, we remark that the corresponding algorithm in the right and bilateral cases can be obtained from the one stated above via trivial modifications. The only nontrivial part is the one marked with • in the algorithm, which respectively becomes:

- **Left:** $c - \gamma = \sum_{i=\mu+1}^{\nu} a_i \alpha_{\lambda_i}(\mathrm{lc}(g_i))$, $\mathbf{T}(g) = \lambda_i \circ \mathbf{T}(g_i), \mu < i \leq \nu$, $h := h - \sum_{i=\mu+1}^{\nu} a_i \lambda_i \star g_i$, $\mu := \nu$;

Figure 2: Canonical Form Algorithms

$(g, \sum_{i=1}^{\mu} a_i\lambda_i \star g_i) :=$ **LeftCanonicalForm**(f, F)

where

$\mathsf{R} := R[\mathcal{T}]$, R a ring with canonical representatives,

$f \in \mathsf{R}^m$, F is the left Gröbner basis of the left module $\mathsf{I} \subset \mathsf{R}^m$,

$g := \mathrm{Can}(f, \mathsf{I}) \in$ **Rep**(I), $a_i \in R \setminus \{0\}, \lambda_i \in \mathcal{T}, g_i \in F$,

$f - g = \sum_{i=1}^{\mu} a_i\lambda_i \star g_i$ is a left weak Gröbner representation in terms of F,

$h := f, \mu := 0, g := 0$

While $h \neq 0$ **do**

Let $c\tau :=$ **M**$(h), \gamma :=$ **Rep**(c, I_τ)

$h := h - \gamma\tau, g := g + \gamma\tau$,

If $c \neq \gamma$, **let** $g_i \in F, \lambda_i \in \mathcal{T}, a_i \in R \setminus \{0\}$:

- $c - \gamma = \sum_{i=\mu+1}^{\nu} a_i\alpha_{\lambda_i}(\mathrm{lc}(g_i))$, $\mathbf{T}(g) = \lambda_i \circ \mathbf{T}(g_i), \mu < i \leq \nu$, $h := h - \sum_{i=\mu+1}^{\nu} a_i\lambda_i \star g_i, \mu := \nu$

- **Right:** $c - \gamma = \sum_{i=\mu+1}^{\nu} \mathrm{lc}(g_i)b_i$, $\mathbf{T}(g) = \mathbf{T}(g_i) \circ \rho_i, \mu < i \leq \nu$, $h := h - \sum_{i=\mu+1}^{\nu} g_i \star \alpha^{-1}_{\mathbf{T}(g_i)}(b_i)\rho_i, \mu := \nu$;
- **Bilateral:** $c - \gamma = \sum_{i=\mu+1}^{\nu} a_i\alpha_{\lambda_i}(\mathrm{lc}(g_i))$, $\mathbf{T}(g) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i, \mu < i \leq \nu$, $h := h - \sum_{i=\mu+1}^{\nu} a_i\lambda_i \star g_i \star \rho_i, \mu := \nu$.

5 Möller's Lifting Theorem

Let R be a not necessarily commutative domain and R be a multivariate Ore extension.

5.1 Valuation

5.1.1 Left (right) case

The validity of Corollary 15 allows to intoduce the groebnerian terminology and, as in the standard theory of commutative polynomial rings over a field [31, § 21.1-2] or a Zacharias ring [54], the ability of imposing a $\mathcal{T}^{(m)}$-valuation on modules over R and its associated graded Ore extension $\mathsf{S} := G(\mathsf{R})$ (see Remark 10).

The only twist w.r.t. the classical theory is that there the ring was coinciding with its associated graded ring; here they coincide as sets and as left R-modules, but as rings have two different multiplications.

Consequently, denoting by $\star$ the one of R and by $*$ the one of S, given a finite basis

$$F := \{g_1, \ldots, g_u\} \subset \mathsf{R}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i\tau_i\mathbf{e}_{l_i} - p_i,$$

with respect to the module $\mathsf{M} := \mathbb{I}_L(F) \subset \mathsf{R}^m$ we need to consider the morphisms

$$\mathfrak{s}_L : \mathsf{S}^u \to \mathsf{S}^m \quad : \quad \mathfrak{s}_L\left(\sum_{i=1}^u h_i e_i\right) := \sum_{i=1}^u h_i * \mathbf{M}(g_i),$$
$$\mathfrak{S}_L : \mathsf{R}^u \to \mathsf{M} \subset \mathsf{R}^m \quad : \quad \mathfrak{S}_L\left(\sum_{i=1}^u h_i e_i\right) := \sum_{i=1}^u h_i \star g_i,$$

where the symbols $\{e_1, \ldots, e_u\}$ denote the common canonical basis of S^u and R^u which, as R-modules, coincide.

We can then consider

- the $\mathcal{T}^{(m)}$-valuation $v : \mathsf{R}^u \to \mathcal{T}^{(m)}$ defined, for each $\sigma := \sum_{i=1}^u h_i e_i \in \mathsf{R}^u \setminus \{0\}$, by

$$v(\sigma) := \max_<\{\mathbf{T}(h_i \star g_i)\} = \max_<\{\mathbf{T}_<(h_i) \circ \mathbf{T}_<(g_i)\} = \max_<\{\mathbf{T}_<(h_i) \circ \tau_i \mathbf{e}_{l_i}\} =: \delta\epsilon$$

  under which we further have $\mathsf{S}^u = G(\mathsf{R}^u)$;

- the corresponding *leading form* $\mathcal{L}_L(\sigma) := \sum_{h \in H} \mathbf{M}(h_h) e_h \in \mathsf{S}^u$ – which is $\mathcal{T}^{(m)}$-homogeneous of $\mathcal{T}^{(m)}$-degree $v(\sigma) = \delta\epsilon$ – where

$$H := \left\{j : \mathbf{T}_<(h_j \star g_j) = \mathbf{T}_<(h_j) \circ \tau_j \mathbf{e}_{l_j} = \delta\epsilon = v(\sigma)\right\}.$$

For each set $S \subset \mathsf{R}^u$, we denote $\mathcal{L}_L\{S\} := \{\mathcal{L}_L(g) : g \in S\} \subset \mathsf{S}^u$.

5.1.2 Bilateral case

Considering R as a left R-module, the adaptation of Möller lifting theorem to the bilateral case requires a few elementary adaptations; given a finite set

$$F := \{g_1, \ldots, g_u\} \subset \mathsf{R}^m,\ g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{l_i} - p_i,$$

and the bilateral module $\mathsf{M} := \mathbb{I}_2(F)$, denote

$$\hat{R} := \{a \in R : ah = a \star h = h \star a,\ \text{for each } h \in \mathsf{R}\}$$

the commutative subring $\hat{R} \subset R$ of R consisting of the elements belonging to the center of R and remark that the subring of R generated by $\mathbf{1}_R$ is a subring of $\hat{R}$ and that $\hat{R}$ is also a subring of the center of the associated graded Ore extension S of R.

Considering both the R-bimodule $\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}}$ and the S-bimodule $\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}}$, which, as sets, coincide, we impose on the bilateral R-module $(\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$, whose canonical basis is denoted $\{e_1, \ldots, e_u\}$ and whose generic element has the shape

$$\sum_i a_i \lambda_i e_{\ell_i} b_i \rho_i,\ a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, 1 \leq \ell_i \leq u,$$

the $\mathcal{T}^{(m)}$-graded structure given by the valuation $v : (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u \to \mathcal{T}$ as

$$v(\sigma) := \max_<\{\mathbf{T}(\lambda_i \star g_{\ell_i} \star \rho_i)\} = \max_<\{\lambda_i * \mathbf{T}(g_{\ell_i}) * \rho_i\} = \max_<\{\lambda_i \circ \tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}}\} =: \delta\epsilon$$

for each

$$\sigma := \sum_i a_i \lambda_i e_{\ell_i} b_i \rho_i \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u \setminus \{0\}$$

so that

$$G\left((\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u\right) = \left(G\left(\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}}\right)\right)^u = (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u$$

and its corresponding $\mathcal{T}^{(m)}$-homogeneous *leading form* is

$$\mathcal{L}_2(\sigma) := \sum_{h \in H} a_h \lambda_h e_{\ell_h} b_h \rho_h \in (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u$$

where $H := \{j : \lambda_j \circ \tau_{\ell_j} \circ \rho_j \mathbf{e}_{l_{\ell_j}} = v(\sigma) = \delta\epsilon\}$; we also denote, for each set $S \subset (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$,

$$\mathcal{L}_2\{S\} := \{\mathcal{L}_2(g) : g \in S\} \subset (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u .$$

We can therefore consider the morphisms

$$\mathfrak{s}_2 : (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u \to \mathsf{S}^m \quad : \quad \mathfrak{s}_2\left(\sum_i a_i \lambda_i e_{\ell_i} b_i \rho_i\right) := \sum_i a_i \lambda_i * \mathbf{M}(g_{\ell_i}) * b_i \rho_i,$$

$$\mathfrak{S}_2 : (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u \to \mathsf{R}^m \quad : \quad \mathfrak{S}_2\left(\sum_i a_i \lambda_i e_{\ell_i} b_i \rho_i\right) := \sum_i a_i \lambda_i \star g_{\ell_i} \star b_i \rho_i.$$

5.1.3 Restricted case

In order to deal with restricted modules, we need simply to adapt and simplify the bilateral case.

Thus, we consider both the left R-modules $R \otimes \mathsf{R}^{\mathrm{op}}$ and $R \otimes \mathsf{S}^{\mathrm{op}}$, which, as sets, coincide, we impose on the bilateral R-module $(R \otimes \mathsf{R}^{\mathrm{op}})^u$, whose canonical basis is denoted $\{e_1, \ldots, e_u\}$ and whose generic element has the shape

$$\sum_i a_i e_{\ell_i} \rho_i, a_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, 1 \leq \ell_i \leq u,$$

the $\mathcal{T}^{(m)}$-graded structure given by the valuation $v : (R \otimes \mathsf{R}^{\mathrm{op}})^u \to \mathcal{T}$ as

$$v(\sigma) := \max_{<}\{\mathbf{T}(g_{\ell_i} \star \rho_i)\} = \max_{<}\{\mathbf{T}(g_{\ell_i}) * \rho_i\} = \max_{<}\{\tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}}\} =: \delta\epsilon$$

for each

$$\sigma := \sum_i a_i e_{\ell_i} \rho_i \in (R \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u \setminus \{0\}$$

so that

$$G\left((R \otimes \mathsf{R}^{\mathrm{op}})^u\right) = \left(G\left(R \otimes \mathsf{R}^{\mathrm{op}}\right)\right)^u = (R \otimes \mathsf{S}^{\mathrm{op}})^u$$

and its corresponding $\mathcal{T}^{(m)}$-homogeneous *leading form* is

$$\mathcal{L}_W(\sigma) := \sum_{h \in H} a_h e_{\ell_h} \rho_h \in (R \otimes \mathsf{S}^{\mathrm{op}})^u$$

where $H := \{j : \tau_{\ell_j} \circ \rho_j \mathbf{e}_{l_{\ell_j}} = v(\sigma) = \delta\epsilon\}$; we also denote, for each set $S \subset (R \otimes \mathsf{R}^{\mathrm{op}})^u$,

$$\mathcal{L}_W\{S\} := \{\mathcal{L}_W(g) : g \in S\} \subset (R \otimes \mathsf{S}^{\mathrm{op}})^u .$$

We can therefore consider the morphisms

$$\mathfrak{s}_W : (R \otimes \mathsf{S}^{\mathrm{op}})^u \to \mathsf{S}^m \quad : \quad \mathfrak{s}_W\left(\sum_i a_i e_{\ell_i} \rho_i\right) := \sum_i a_i \mathbf{M}(g_{\ell_i}) * \rho_i,$$

$$\mathfrak{S}_W : (R \otimes \mathsf{R}^{\mathrm{op}})^u \to \mathsf{R}^m \quad : \quad \mathfrak{S}_W\left(\sum_i a_i e_{\ell_i} \rho_i\right) := \sum_i a_i g_{\ell_i} \star \rho_i.$$

5.2 Lifting Theorem

Definition 33. With the notation above

- for a (left, right, bilateral, restricted) R-module N, a set $B \subset \mathsf{N}$ is called a (left, right, bilateral, restricted) *standard basis* if

$$\mathbb{I}(\mathcal{L}\{B\}) = \mathbb{I}(\mathcal{L}\{\mathsf{N}\});$$

- for each $h \in \mathsf{N}$ a representation

$$h = \sum_i l_i \star g_i : l_i \in \mathsf{R}, g_i \in B,$$

  is called a *left standard representation* in R in terms of B iff

$$v(h) \geq v(l_i \star g_i) = \mathbf{T}(l_i) \circ \mathbf{T}(g_i) \text{ for each } i;$$

- for each $h \in \mathsf{N}$ a representation

$$h = \sum_i g_i \star r_i : r_i \in \mathsf{R}, g_i \in B,$$

  is called a *right standard representation* in R in terms of B iff

$$v(h) \geq v(g_i \star r_i) = \mathbf{T}(g_i) \circ \mathbf{T}(r_i) \text{ for each } i;$$

- for each $h \in \mathsf{N}$ a representation

$$h = \sum_i a_i \lambda_i \star g_{\ell_i} \star b_i \rho_i : a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, g_{\ell_i} \in B,$$

  is called a *bilateral standard representation* in R in terms of B iff

$$v(h) \geq v(\lambda_i \star g_{\ell_i} \star \rho_i) = \lambda_i \circ v(g_{\ell_i}) \circ \rho_i, \text{ for each } i;$$

– for each $h \in \mathsf{N}$ a representation

$$h = \sum_i a_i g_{\ell_i} \star \rho_i : a_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_{\ell_i} \in B,$$

is called a *restricted standard representation* in R in terms of B iff

$$v(h) \geq v(g_{\ell_i} \star \rho_i) = v(g_{\ell_i}) \circ \rho_i, \text{ for each } i;$$

– if $u \in \ker(\mathfrak{s})$ is $\mathcal{T}^{(m)}$-homogeneous and $U \in \ker(\mathfrak{S})$ is such that $u = \mathcal{L}(U)$, we say that u *lifts* to U, or U is a *lifting* of u, or simply u *has a lifting*;

– a (left, right, bilateral, restricted) *Gebauer–Möller set* for B is any $\mathcal{T}^{(m)}$-homogeneous basis of $\ker(\mathfrak{s})$;

– for each $\mathcal{T}^{(m)}$-homogeneous element $\sigma \in \mathsf{R}^u$, we say that $\mathfrak{S}_L(\sigma)$ has a left *quasi-Gröbner representation* in terms of B if it can be written as $\mathfrak{S}_L(\sigma) = \sum_{i=1}^u l_i \star g_i$ with $v(\sigma) > \mathbf{T}(l_i \star g_i) = \mathbf{T}(l_i) \circ \mathbf{T}(g_i)$ for each i.

– for each $\mathcal{T}^{(m)}$-homogeneous element $\sigma \in \mathsf{R}^u$, we say that $\mathfrak{S}_R(\sigma)$ has a right *quasi-Gröbner representation* in terms of B if it can be written as $\mathfrak{S}_R(\sigma) = \sum_{i=1}^u g_i \star r_i$ with $v(\sigma) > \mathbf{T}(g_i \star r_i) = \mathbf{T}(g_i) \circ \mathbf{T}(r_i)$ for each i.

– for each $\mathcal{T}^{(m)}$-homogeneous element $\sigma \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$, we say that $\mathfrak{S}_2(\sigma)$ has a bilateral *quasi-Gröbner representation* in terms of B if it can be written as

$$\mathfrak{S}_2(\sigma) = \sum_i a_i \lambda_i \star g_{\ell_i} \star b_i \rho_i : a_i, b_i \in R \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, g_{\ell_i} \in B$$

with $v(\sigma) > \lambda_i \circ \mathbf{T}(g_{\ell_i}) \circ \rho_i$ for each i.

– for each $\mathcal{T}^{(m)}$-homogeneous element $\sigma \in (R \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$, we say that $\mathfrak{S}_W(\sigma)$ has a restricted *quasi-Gröbner representation* in terms of B if it can be written as

$$\mathfrak{S}_W(\sigma) = \sum_i a_i g_{\ell_i} \star \rho_i : a_i \in R \setminus \{0\}, \rho_i \in \mathcal{T}, g_{\ell_i} \in B$$

with $v(\sigma) > \mathbf{T}(g_{\ell_i}) \circ \rho_i$ for each i. □

Remark 34. Note that each left Gröbner representation of $\mathfrak{S}_L(\sigma)$ in terms of B gives also a left quasi-Gröbner representation since $\mathbf{T}(l_i) \circ \mathbf{T}(g_i) \leq \mathbf{T}(\mathfrak{S}_L(\sigma)) < v(\sigma)$; on the other side, a left quasi-Gröbner representation grants only $\mathbf{T}(l_i) \circ \mathbf{T}(g_i) < v(\sigma)$ but not necessarily $\mathbf{T}(l_i) \circ \mathbf{T}(g_i) \leq \mathbf{T}(\mathfrak{S}_L(\sigma))$, since in principle we could have $\mathbf{T}(\mathfrak{S}_L(\sigma)) < \mathbf{T}(l_i) \circ \mathbf{T}(g_i) < v(\sigma)$ so that we don't necessarily obtain a left Gröbner representation of the S-polynomial $\mathfrak{S}_L(\sigma)$.

This relaxation was introduced by Gebauer and Möller in their reformulation of Buchberger Theory for polynomial rings over a field [19]; in that setting, it allowed to better remove useless S-pairs and thus granted a more efficient reformulation of the algorithm; in the more general setting we are considering now, viz polynomials over *rings*, it becomes essential also for a smooth reformulation of the theory.

□

Remark 35. Observe that if $\sigma := \sum_{j=1}^{u} h_j e_j \in \ker(\mathfrak{S}_L)$ then denoting

$$\delta\epsilon := v(\sigma) \text{ and } H := \left\{ j, 1 \leq j \leq u : \mathbf{T}(h_j) \circ \mathbf{T}(g_j) = \delta\epsilon \right\},$$

its *leading form* $\mathcal{L}_L(\sigma) := \sum_{j=1}^{u} d_j \lambda_j e_j \in \mathsf{S}^u$ is $\mathcal{T}^{(m)}$-homogeneous of $\mathcal{T}^{(m)}$-degree $v(\sigma) := \delta\epsilon \in \mathcal{T}^{(m)}$, satisfies

- $0 \neq d_j \iff j \in H$ and $\mathbf{M}(h_j) = d_j \lambda_j$,
- $\sum_{j=1}^{u} d_j \lambda_j * \mathbf{M}(g_j) = \sum_{j \in H} (d_j \lambda_j) * (c_j \tau_j \mathbf{e}_{l_j}) = \left(\sum_{j \in H} \left(d_j \alpha_{\lambda_j}(c_j) \right) \cdot \left(\lambda_j \tau_j \right) \right) \epsilon = 0$,
- $\sum_{j \in H} d_j \alpha_{\lambda_j}(\mathrm{lc}(g_j)) = 0$ and $\lambda_j \circ \mathbf{T}(g_j) = \delta\epsilon$ for each $j \in H$, so that in particular
- $\epsilon = \mathbf{e}_{l_j}$ for each $j \in H$,

and belongs to $\ker(\mathfrak{s}_L)$.

Adapting Remarks 34 and 35 as done for Definition 33, one can obtain the analogous remarks for the right, bilateral and restricted case.

Theorem 36 (Möller-Pritchard; Lifting Theorem)**.** [35]
With the present notation and denoting $\mathfrak{GM}(F)$ any Gebauer–Möller set for $F \subset \mathsf{R}$, the following conditions are equivalent:

1. *F is a Gröbner basis of $\mathbb{I}(F)$;*
2. *$f \in \mathbb{I}(F) \iff f$ has a Gröbner representation in terms of F;*
3. *for each $\sigma \in \mathfrak{GM}(F)$, the S-polynomial $\mathfrak{S}(\sigma)$ has a quasi-Gröbner representation;*
4. *each $\sigma \in \mathfrak{GM}(F)$ has a lifting* $\mathrm{lift}(\sigma)$*;*
5. *each $\mathcal{T}^{(m)}$-homogeneous element $u \in \ker(\mathfrak{s})$ has a lifting* $\mathrm{lift}(u)$.

Proof.
We prove the statement only in the bilateral case, leaving to the reader the adaptations to the right, left and restricted cases.

(1) $\implies$ (2) Let $f \in \mathbb{I}(F)$; by assumption

$$\mathbf{M}(f) = \sum_{i=1}^{\mu} a_i \lambda_i * \mathbf{M}(g_{\ell_i}) * b_i \rho_i$$

where $\sum_{i=1}^{\mu} a_i \lambda_i e_{\ell_i} b_i \rho_i \in (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u$ is $\mathcal{T}^{(m)}$-homogeneous of $\mathcal{T}^{(m)}$-degree $\mathbf{T}(f)$.
Therefore $g := f - \sum_{i=1}^{\mu} a_i \lambda_i \star g_{\ell_i} \star b_i \rho_i \in \mathbb{I}(F)$ and $\mathbf{T}(g) < \mathbf{T}(f)$.
Thus, the claim follows by induction since $<$ is a well-ordering.

(2) $\implies$ (3) $\mathfrak{S}_2(\sigma) \in \mathbb{I}(F)$ and $\mathbf{T}(\mathfrak{S}_2(\sigma)) < v(\sigma)$.

(3) $\Longrightarrow$ (4) Let

$$\mathfrak{S}_2(\sigma) = \sum_{i=1}^{\mu} a_i\lambda_i \star g_{\ell_i} \star b_i\rho_i, v(\sigma) > \lambda_i \circ \tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}}$$

be a bilateral quasi-Gröbner representation in terms of F; then

$$\mathrm{lift}(\sigma) := \sigma - \sum_{i=1}^{\mu} a_i\lambda_i e_{\ell_i} b_i\rho_i$$

is the required lifting of σ.

(4) $\Longrightarrow$ (5) Let $u := \sum_i a_i\lambda_i e_{\ell_i} b_i\rho_i \in (\mathsf{S} \otimes_{\hat{R}} \mathsf{S}^{\mathrm{op}})^u$, $\lambda_i \circ \tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}} = v(u)$, be a $\mathcal{T}^{(m)}$-homogeneous element in $\ker(\mathfrak{s}_2)$ of $\mathcal{T}^{(m)}$-degree $v(u)$.

Then there are $\lambda_\sigma, \rho_\sigma \in \mathcal{T}, a_\sigma, b_\sigma \in R \setminus \{0\}$, for which

$$u = \sum_{\sigma \in \mathfrak{GM}(F)} a_\sigma\lambda_\sigma * \sigma * b_\sigma\rho_\sigma, \lambda_\sigma \circ v(\sigma) \circ \rho_\sigma = v(u).$$

For each $\sigma \in \mathfrak{GM}(F)$ denote

$$\bar{\sigma} := \sigma - \mathrm{lift}(\sigma) = \mathcal{L}_2(\mathrm{lift}(\sigma)) - \mathrm{lift}(\sigma) := \sum_{i=1}^{\mu_\sigma} a_{i\sigma}\lambda_{i\sigma} e_{\ell_{i\sigma}} b_{i\sigma}\rho_{i\sigma} \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$$

and remark that $\lambda_{i\sigma} \circ \tau_{\ell_{i\sigma}} \circ \rho_{i\sigma}\mathbf{e}_{l_{\ell_{i\sigma}}} \leq v(\bar{\sigma}) < v(\sigma)$ and $\mathfrak{S}_2(\bar{\sigma}) = \mathfrak{S}_2(\sigma)$.

It is sufficient to define

$$\mathrm{lift}(u) := \sum_{\sigma \in \mathfrak{GM}(F)} a_\sigma\lambda_\sigma \star \mathrm{lift}(\sigma) \star b_\sigma\rho_\sigma, \text{ and } \bar{u} := \sum_{\sigma \in \mathfrak{GM}(F)} a_\sigma\lambda_\sigma \star \bar{\sigma} \star b_\sigma\rho_\sigma$$

to obtain

$$\mathrm{lift}(u) = u - \bar{u}, \mathcal{L}_2(\mathrm{lift}(u)) = u, \mathfrak{S}_2(\bar{u}) = \mathfrak{S}_2(u), \mathfrak{S}_2(\mathrm{lift}(u)) = 0.$$

(5) $\Longrightarrow$ (1) Let $g \in \mathbb{I}(F)$, so that there are $\lambda_i, \rho_i \in \mathcal{T}, a_i, b_i \in R \setminus \{0\}, 1 \leq \ell_i \leq u$, such that $\sigma_1 := \sum_{i=1}^{\mu} a_i\lambda_i e_{\ell_i} b_i\rho_i \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$ satisfies

$$g = \mathfrak{S}_2(\sigma_1) = \sum_{i=1}^{\mu} a_i\lambda_i \star g_{\ell_i} \star b_i\rho_i.$$

Denoting $H := \{i : \lambda_i \circ \mathbf{T}(g_{\ell_i}) \circ \rho_i = \lambda_i \circ \tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}} = v(\sigma_1)\}$, then either

- $v(\sigma_1) = \mathbf{T}(g)$ so that, for each $i \in H$, $\mathbf{M}(a_i\lambda_i \star \mathbf{M}(g_{\ell_i}) \star b_i\rho_i) = a_i\lambda_i * \mathbf{M}(g_{\ell_i}) * b_i\rho_i$ and

$$\mathbf{M}(g) = \sum_{i \in H} a_i\lambda_i * \mathbf{M}(g_{\ell_i}) * b_i\rho_i \in \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\},$$

and we are through, or

– $\mathbf{T}(g) < v(\sigma_1)$, in which case $0 = \sum_{i\in H} a_i\lambda_i * \mathbf{M}(g_{\ell_i}) * b_i\rho_i = \mathfrak{s}_2(\mathcal{L}_2(\sigma_1))$ and the $\mathcal{T}^{(m)}$-homogeneous element $\mathcal{L}_2(\sigma_1) \in \ker(\mathfrak{s}_2)$ has a lifting

$$U := \mathcal{L}_2(\sigma_1) - \sum_{j=1}^{\nu} a_j\lambda_j e_{\ell_j} b_j\rho_j \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$$

with

$$\sum_{j=1}^{\nu} a_j\lambda_j \star g_{\ell_j} \star b_j\rho_j = \sum_{i\in H} a_i\lambda_i \star g_{\ell_i} \star b_i\rho_i \text{ and } \lambda_j \circ \tau_{\ell_j} \circ \rho_j \mathbf{e}_{l_{\ell_j}} < v(\sigma_1)$$

so that $g = \mathfrak{S}_2(\sigma_2)$ and $v(\sigma_2) < v(\sigma_1)$ holds for

$$\sigma_2 := \sum_{i\notin H} a_i\lambda_i e_{\ell_i} b_i\rho_i + \sum_{j=1}^{\nu} a_j\lambda_j e_{\ell_j} b_j\rho_j \in (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$$

and the claim follows by the well-orlderedness of $<$.

□

Theorem 37 (Janet—Schreyer)**.** *[20, 47, 48]*
With the same notation the equivalent conditions (1-5) imply that

6. $\{\mathrm{lift}(\sigma) : \sigma \in \mathfrak{GM}(F)\}$ *is a standard basis of* $\ker(\mathfrak{S})$.

Proof. (4) $\implies$ (6) Let $\sigma_1 := \sum_{i=1}^{\mu} a_i\lambda_i e_{\ell_i} b_i\rho_i \in \ker(\mathfrak{S}_2) \subset (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$.

Denoting $H := \{i : \lambda_i \circ \tau_{\ell_i} \circ \rho_i \mathbf{e}_{l_{\ell_i}} = v(\sigma_1)\}$, we have

$$\mathcal{L}_2(\sigma_1) = \sum_{i\in H} a_i\lambda_i e_{\ell_i} b_i\rho_i \in \ker(\mathfrak{s}_2)$$

and there is a $\mathcal{T}^{(m)}$-homogeneous representation

$$\mathcal{L}_2(\sigma_1) = \sum_{\sigma\in\mathfrak{GM}(F)} a_\sigma\lambda_\sigma * \sigma * b_\sigma\rho_\sigma, \lambda_\sigma \circ v(\sigma) \circ \rho = v(\sigma_1)$$

with $\lambda_\sigma, \rho_\sigma \in \mathcal{T}, a_\sigma, b_\sigma \in R \setminus \{0\}$.

Then

$$\begin{aligned}
\sigma_2 &:= \sigma_1 - \sum_{\sigma\in\mathfrak{GM}(F)} a_\sigma\lambda_\sigma \star \mathrm{lift}(\sigma) \star b_\sigma\rho_\sigma \\
&= \sigma_1 - \sum_{\sigma\in\mathfrak{GM}(F)} a_\sigma\lambda_\sigma \star (\sigma - \bar{\sigma}) \star b_\sigma\rho_\sigma \\
&= \sigma_1 - \mathcal{L}_2(\sigma_1) + \sum_{\sigma\in\mathfrak{GM}(F)} a_\sigma\lambda_\sigma \star \bar{\sigma} \star b_\sigma\rho_\sigma \\
&= \sum_{i\notin H} a_i\lambda_i e_{\ell_i} b_i\rho_i \\
&+ \sum_{\sigma\in\mathfrak{GM}(F)} \sum_{i=1}^{\mu_\sigma} \Big((a_\sigma\alpha_{\lambda_\sigma}(a_{i\sigma})) \cdot (\lambda_\sigma \circ \lambda_{i\sigma})\Big) e_{\ell_{i\sigma}} \Big(\Big(b_{i\sigma}\alpha_{\rho_{i\sigma}}(b_\sigma)\Big) \cdot (\rho_{i\sigma} \circ \rho_\sigma)\Big)
\end{aligned}$$

satisfies both $\sigma_2 \in \ker(\mathfrak{S}_2)$ and $v(\sigma_2) < v(\sigma_1)$; thus the claim follows by induction.

□

Example 38. Let us consider the ring of Example 17 and three elements $f_1, f_2, f_3 \in \mathsf{R}$ with

$$\mathbf{M}(f_1) = (5x-1)Y_1Y_2^2Y_3^2, \mathbf{M}(f_2) = (5x-1)Y_1^2Y_2Y_3^2, \mathbf{M}(f_3) = (5x-1)Y_1^2Y_2^2Y_3.$$

Under the natural $\mathcal{T}$-pseudovaluation on R^3, an element

$$\sigma := \left(\alpha Y_1^{\alpha_1}Y_2^{\alpha_2}Y_3^{\alpha_3}, \beta Y_1^{\beta_1}Y_2^{\beta_2}Y_3^{\beta_3}, \gamma Y_1^{\gamma_1}Y_2^{\gamma_2}Y_3^{\gamma_3}\right) \in \mathsf{S}^3 \tag{7}$$

is homogeneous of $\mathcal{T}$-degree $Y_1^{a+2}Y_2^{b+2}Y_3^{c+2}$ iff

$$\alpha_1 - 1 = \beta_1 = \gamma_1 =: a, \alpha_2 = \beta_2 - 1 = \gamma_2 =: b, \alpha_3 = \beta_3 = \gamma_3 - 1 =: c.$$

Let us now specialize ourselves to the case $a = b = c = 0$ and consider the $\mathbb{Z}[x]$-module of the homogeneous syzygies of $\mathcal{T}$-degree $Y_1^2Y_2^2Y_3^2$; setting $y = 5x$, (7) is a syzygy in $\ker(\mathfrak{s}_L)$ iff

$$\begin{aligned} 0 &= \mathfrak{s}_L(\sigma) \\ &= \alpha Y_1 * \mathbf{M}(f_1) + \beta Y_2 * \mathbf{M}(f_2) + \gamma Y_3 * \mathbf{M}(f_3) \\ &= \left(\alpha(y^2-1) + \beta(y^3-1) + \gamma(y^4-1)\right) Y_1^2Y_2^2Y_3^2. \end{aligned}$$

A minimal left Gebauer-Möller set consists of

$$\sigma_1 := (-(y^2+y+1)Y_1, (y+1)Y_2, 0) \text{ and } \sigma_2 := (-(y^2+1)Y_1, 0, Y_3).$$

In fact a generic syzygy (7) satisfies

$$\alpha(y+1) + \beta(y^2+y+1) + \gamma(y^2+1)(y+1) = 0$$

so that $(y+1) \mid \beta$ and setting $\beta = (y+1)\delta$ we have $\alpha = -\delta(y^2+y+1) - \gamma(y^2+1)$ whence

$$\sigma := \left(\left(-\delta(y^2+y+1) - \gamma(y^2+1)\right) Y_1, (y+1)\delta Y_2, \gamma Y_3\right) = \delta\sigma_1 + \gamma\sigma_2.$$

Remark 39. We can consider also the homogeneous syzygy of $\mathcal{T}$-degree $Y_1^2Y_2^2Y_3^2$

$$\sigma_3 := (0, -(y^2+1)(y+1)Y_2, (y^2+y+1)Y_3) = -(y^2+1)\sigma_1 + (y^2+y+1)\sigma_2.$$

Moreover, since

$$1 = (y^2+y+1) - y(y+1) = (y^3+y^2+y+1) - y(y^2+y+1)$$

setting

$$\varsigma_A := (-yY_1, Y_2, 0) \in \mathsf{S}^3, \varsigma_B := (0, -yY_2, Y_3) \in \mathsf{S}^3$$

we have

$$\mathfrak{s}_L(\varsigma_A) = \mathfrak{s}_L(\varsigma_B) = (y-1)Y_1^2Y_2^2Y_3^2;$$

note that

$$\varsigma_A - \varsigma_B := (-yY_1, (y+1)Y_2, -Y_3) = \sigma_1 - \sigma_2 \in \ker(\mathfrak{s}_L).$$

□

Example 38 (cont.). Setting now $\tau := Y_1^a Y_2^b Y_3^c$ and $z := y^{2^a 3^b 4^c}$, for the syzygy (7) we have

$$\begin{aligned} 0 &= \mathfrak{s}_L(\sigma) \\ &= \alpha\tau Y_1 * \mathbf{M}(f_1) + \beta\tau Y_2 * \mathbf{M}(f_2) + \gamma\tau Y_3 * \mathbf{M}(f_3) \\ &= \left(\alpha\tau * (y^2-1) + \beta\tau * (y^3-1) + \gamma\tau * (y^4-1)\right) Y_1^2 Y_2^2 Y_3^2. \\ &= \left(\alpha(z^2-1) + \beta(z^3-1) + \gamma(z^4-1)\right) Y_1^2 Y_2^2 Y_3^2 \tau \end{aligned}$$

whence

$$\alpha = -\delta(z^2+z+1) - \gamma(z^2+1), \quad \beta = (z+1)\delta$$

and

$$\sigma := \delta\tau * \sigma_1 + \gamma\tau * \sigma_2.$$

Thus, $\{\sigma_1, \sigma_2\}$ is a minimal basis of $\ker(\mathfrak{s}_L)$.

6 Gröbner basis Computation for Multivariate Ore Extensions of Zacharias Domains

We recall the definition of Zacharias ring [54], [31, §26.1], [32].

Definition 40. A ring R with identity is called a (left) *Zacharias ring* if it satisfies the following properties:

(a). R is a noetherian ring;

(b). there is an algorithm which, for each $c \in R^m$, $C := \{c_1, \dots c_t\} \subset R^m \setminus \{0\}$, allows to decide whether $c \in \mathbb{I}_L(C)$ in which case it produces elements $d_i \in R : c = \sum_{i=1}^t d_i c_i$;

(c). there is an algorithm which, given $\{c_1, \dots c_t\} \subset R^m \setminus \{0\}$, computes a finite set of generators for the left syzygy R-module $\left\{(d_1, \cdots, d_t) \in R^t : \sum_{i=1}^t d_i c_i = 0\right\}$.

Note that [35] for a ring R with identity which satisfies (a) and (b), (c) is equivalent to

(d). there is an algorithm which, given $\{c_1, \dots c_s\} \subset R^m \setminus \{0\}$, computes a finite basis of the ideal

$$\mathbb{I}_L(\{c_i : 1 \le i < s\}) : \mathbb{I}_L(c_s).$$

If R has canonical representatives, we improve the computational assumptions of Zacharias rings, requiring also the following property:

(e). there is an algorithm which, given an element $c \in R^m$ and a left module $\mathsf{J} \subset R^m$, computes the unique canonical representative $\mathbf{Rep}(c, \mathsf{J})$. □

If R is a left Zacharias domain, the three algorithms proposed by Möller [35] for computing Gröbner bases in the polynomial ring over R can be easily adapted to multivariate Ore extensions of Zacharias domains, provided that each α_i, and therefore each α_τ, is an automorphism.

6.1 First algorithm

Still considering a finite basis

$$F := \{g_1, \dots, g_u\} \subset \mathsf{R}^m,\ g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{l_i} - p_i,$$

of the module $\mathsf{M} := \mathbb{I}_L(F)$ and denoting

- $\mathfrak{H}(F) := \{\{i_1, i_2, \dots, i_r\} \subseteq \{1, \dots, u\} : l_{i_1} = \cdots = l_{i_r}\}$;
- for each $H := \{i_1, i_2, \dots, i_r\} \in \mathfrak{H}(F)$,
  - $\varepsilon_H := \mathbf{e}_{l_{i_1}} = \cdots = \mathbf{e}_{l_{i_r}}$,
  - $\tau_H := \operatorname{lcm}(\tau_i : i \in H)$,
  - for each $I \subset H$,
    - $\tau_{H,I} := \frac{\tau_H}{\tau_I}$,
    - $\alpha_{H,I} : R \to R$ the morphism $\alpha_{\tau_{H,I}}$;[3]
  - $\mathbf{T}(H) := \tau_H \varepsilon_H$,

  and, if R is a PID,
  - $c_H := \operatorname{lcm}(\alpha_{H,i}(c_i) : i \in H)$,
  - $\mu(H) := c_H \tau_H$ and
  - $\mathbf{M}(H) = c_H \mathbf{T}(H) = c_H \tau_H \varepsilon_H = \mu(H) \varepsilon_H$;
- $\mathsf{T} := \{\mathbf{T}(H) : H \in \mathfrak{H}(F)\}$;
- for any $\mathsf{m} = \delta\epsilon \in \mathsf{T}$,
  - for each $i, 1 \le i \le u, t_i(\mathsf{m}) := \begin{cases} \frac{\delta}{\tau_i} & \text{if } \mathbf{T}(g_i) \mid \mathsf{m}, \\ 1 & \text{otherwise;} \end{cases}$
  - $v(\mathsf{m}) = (v(\mathsf{m})_1, \dots, v(\mathsf{m})_u) \in R^u$ the vector such that
$$v(\mathsf{m})_i := \begin{cases} \alpha_{t_i(\mathsf{m})}(\operatorname{lc}(g_i)) & \text{if } \mathbf{T}(g_i) \mid \mathsf{m}, \\ 0 & \text{otherwise;} \end{cases}$$
  - $C(\mathsf{m}) \subset R^u$ a finite basis of the syzygy module
$$\operatorname{Syz}_L(v(\mathsf{m})_1, \dots, v(\mathsf{m})_u) := \left\{(d_1, \dots, d_u) \in R^u : \sum_{i=1}^{u} d_i v(\mathsf{m})_i = 0\right\};$$
  - $S(\mathsf{m}) := \{(d_1 t_1(\mathsf{m}), \dots, d_u t_u(\mathsf{m})) : (d_1, \dots, d_u) \in C(\mathsf{m})\}$;
- $\mathcal{S}(F) := \bigcup_{\mathsf{m} \in \mathsf{T}} S(\mathsf{m})$;
- $\mathcal{S}'(F) \subset \mathcal{S}(F)$ any subset satisfying

[3] If $I = \{i\}$ we will write $\alpha_{H,i}$ and $\tau_{H,i}$ instead of $\alpha_{H,I}$ and $\tau_{H,I}$.

– for each $\sigma \in \mathcal{S}(F) \setminus \mathcal{S}'(F)$ exist $\sigma_j \in \mathcal{S}'(F), d_j \in R, \tau_j \in \mathcal{T}$, such that $\sigma = \sum_j d_j \tau_j * \sigma_j$;

– $\mathcal{R}(F) := \{\sum_i m_i \star g_i : (m_1, \ldots, m_u) \in \mathcal{S}'(F)\}$,

we have that (*cf.* [35], [31, Theorem 26.1.4])

Lemma 41. *$\mathcal{S}(F)$ is a left Gebauer–Möller set for F.*

Proof. Let us consider a generic $\mathcal{T}^{(m)}$-homogeneus element

$$\sigma := \sum_{i=1}^{u} a_i \lambda_i e_i \in \mathsf{R}^u \setminus \{0\},$$

with $a_i \in R, \lambda_i \in \mathcal{T}, v(\sigma) := \tau\epsilon$, and $a_i \neq 0 \implies \lambda_i \tau_i = \tau, \epsilon = \mathbf{e}_{l_i}$, and assume that it is a left syzygy in $\ker(\mathsf{s}_L)$.

Denoting $I := \{i \leq u : a_i \neq 0\}$ and setting $\mathsf{m} := \delta\epsilon := \operatorname{lcm}\{\mathbf{T}(g_i) : i \in I\} \mid v(\sigma)$, there is $\upsilon \in \mathcal{T} : \upsilon\delta = \tau$. With the present notation we also have $\delta = t_i(\mathsf{m})\tau_i$; thus $\upsilon t_i(\mathsf{m})\tau_i = \upsilon\delta = \lambda_i\tau_i$ and $\lambda_i = \upsilon t_i(\mathsf{m})$. We also have

$$0 = \sum_{i=1}^{u} a_i \alpha_{\lambda_i}(\operatorname{lc}(g_i))$$

so that

$$0 = \alpha_\upsilon^{-1}\left(\sum_{i=1}^{u} a_i \alpha_{\lambda_i}(\operatorname{lc}(g_i))\right) = \sum_{i=1}^{u} \alpha_\upsilon^{-1}(a_i)\alpha_{t_i(\mathsf{m})}(\operatorname{lc}(g_i))$$

and $(\alpha_\upsilon^{-1}(a_1), \ldots, \alpha_\upsilon^{-1}(a_u)) \in \operatorname{Syz}_L(v(\mathsf{m})_1, \ldots, v(\mathsf{m})_u)$.

Therefore, if we enumerate as

$$(d_{11}, \ldots, d_{1u}), \ldots, (d_{v1}, \ldots, d_{vu})$$

the elements of a basis of $C(\mathsf{m})$ and we denote $\mathsf{s}_j := \sum_{i=1}^{u} d_{ji} t_i(\mathsf{m}) e_i$, $1 \leq j \leq v$, those of $S(\mathsf{m})$, we have $(\alpha_\upsilon^{-1}(a_1), \ldots, \alpha_\upsilon^{-1}(a_u)) = \sum_{j=1}^{v} b_j (d_{j1}, \ldots, d_{ju})$ for suitable $b_j \in R$ and

$$\begin{aligned}
\sigma &= \sum_{i=1}^{u} a_i \lambda_i e_i \\
&= \sum_{i=1}^{u} a_i \upsilon t_i(\mathsf{m}) e_i \\
&= \sum_{i=1}^{u} \upsilon * \alpha_\upsilon^{-1}(a_i) t_i(\mathsf{m}) e_i \\
&= \upsilon * \sum_{i=1}^{u} \sum_{j=1}^{v} b_j d_{ji} t_i(\mathsf{m}) e_i \\
&= \sum_{j=1}^{v} \alpha_\upsilon(b_j)\upsilon * \left(\sum_{i=1}^{u} d_{ji} t_i(\mathsf{m}) e_i\right) \\
&= \sum_{j=1}^{v} \alpha_\upsilon(b_j)\upsilon * \mathsf{s}_j.
\end{aligned}$$

□

Corollary 42. *The following holds:*

1. *$\mathcal{S}'(F)$ is a left Gebauer–Möller set for F.*
2. *F is a left Gröbner basis of the module it generates iff each $h \in \mathcal{R}(F)$ has a left Gröbner representation in terms of F.* □

Example 43. If we consider the ring of Example 17 as a left $\mathbb{Z}[x]$-module endowed with the Γ-pseudovaluation, $\Gamma = \{Y_1^{a_1}Y_2^{a_2}Y_3^{a_3} : (a_1, a_2, a_1) \in \mathbb{N}^3\}$, we obtain a similar solution as the one described in Example 38 .

Expressing each $\mathbf{M}(f_i)$ as $\mathbf{M}(f_i) = \mathrm{lc}(f_i)\mathbf{T}(f_i)$, according Zacharias approach we need to compute a syzygy basis in $\mathbb{Z}[x]$ among $\alpha_{Y_1}(\mathrm{lc}(f_1)) = (y^2 - 1)$, $\alpha_{Y_2}(\mathrm{lc}(f_2)) = (y^3 - 1)$ and $\alpha_{Y_3}(\mathrm{lc}(f_3)) = (y^4 - 1)$; the natural solutions $(-(y^2 + y + 1), (y + 1), 0)$, $(-(y^2 - 1), 0, 1)$ produce σ_1 and σ_2.

Example 44. Let us now specialize the ring of Example 14 to the case

$$n = 3, e_1 = e_2 = e_3 = 1, c_1 = 20, c_2 = 6, c_3 = 15,$$

and let us consider four elements $f_1, f_2, f_3, f_4 \in \mathsf{R}$ with

$$\mathbf{M}(f_1) = xY_1Y_2^3Y_3^2, \mathbf{M}(f_2) = x^2Y_1^2Y_2Y_3^2, \mathbf{M}(f_3) = xY_1^2Y_2^3Y_3, \mathbf{M}(f_4) = xY_1^2Y_2^2Y_3^2.$$

We have

$$\mathsf{T} = \{Y_1Y_2^3Y_3^2, Y_1^2Y_2Y_3^2, Y_1^2Y_2^2Y_3^2, Y_1^2Y_2^3Y_3, Y_1^2Y_2^3Y_3^2\},$$

and

m	$(t_1(\mathsf{m}), \ldots, t_4(\mathsf{m}))$	$\nu(\mathsf{m})$
$Y_1Y_2^3Y_3^2$	$(1, 0, 0, 0)$	$(x, 0, 0, 0)$
$Y_1^2Y_2Y_3^2$	$(0, 1, 0, 0)$	$(0, x^2, 0, 0)$
$Y_1^2Y_2^2Y_3^2$	$(0, Y_2, 0, 1)$	$(0, 6^2x^2, 0, x)$
$Y_1^2Y_2^3Y_3$	$(0, 0, 1, 0)$	$(0, 0, x, 0)$
$Y_1^2Y_2^3Y_3^2$	(Y_1, Y_2^2, Y_3, Y_2)	$(20x, 6^4x^2, 15x, 6x)$,

Denoting

$$\begin{aligned} b(1,3) &:= (-3Y_1, 0, 4Y_3, 0), \\ b(2,4) &:= (0, -Y_2, 0, 6^2x), \\ b(3,4) &:= (0, 0, -2Y_3, 0, 5Y_2) \end{aligned}$$

we have $S(Y_1^2Y_2^2Y_3^2) = \{b(2,4)\}$ and, since

$$Y_2 * b(2,4) = (0, -Y_2^2, 0, 6^2Y_2 * x) = (0, -Y_2^2, 0, 6^3xY_2)$$

we can take $S(Y_1^2Y_2^3Y_3^2) = \{b(1,3), Y_2 * b(2,4), b(3,4)\}$; thus

$$\mathcal{S}' := \{b(1,3), b(2,4), b(3,4)\}$$

is the required Gebauer–Möller set. □

6.2 Second algorithm

Möller [35] proposed also an (essentially equivalent) alternative computation: for any $s, 1 \leq s \leq u$, let us consider the syzygy module

$$\mathcal{S}_s := \left\{ (h_1, \ldots, h_s) : \sum_{i=1}^{s} h_i \star \mathbf{M}(g_i) = 0 \right\} \subset \mathsf{R}^s$$

and let us compute $\mathcal{S}(F) = \mathcal{S}_u$ by inductively extending $\mathcal{S}_{s-1}$ to $\mathcal{S}_s$, the inductive seed being $\mathcal{S}_1 = \emptyset$.

A direct application of the property (d) of a Zacharias ring allows to compute a Gebauer-Möller set via

Definition 45. A subset $H \subset \{1, \ldots, s\} \cap \mathfrak{H}(F)$, $s \leq u$, is said to be

maximal for a term $\delta\epsilon \in \mathcal{T}^{(m)}$ if $H = \{i, 1 \leq i \leq s : \tau_i \mid \delta, \mathbf{e}_{l_i} = \epsilon\}$,

basic if $s \in H$ and H is maximal for $\mathbf{T}(H)$.

For a basic subset $H \subset \{1, \ldots, s\} \cap \mathfrak{H}(F)$, denote $H^\times := H \setminus \{s\}$.
For any

$$d_s \in \mathbb{I}_L(\{\alpha_{H,i}(c_i) : i \in H^\times\}) : \mathbb{I}_L(\alpha_{H,s}(c_s)),$$

a *syzygy associated to H and* d_s is a $\mathcal{T}^{(m)}$-homogeneous syzygy

$$\sum_{i \in H^\times} d_i \frac{\tau_H}{\tau_i} e_i + d_s \frac{\tau_H}{\tau_s} e_s \in \mathcal{S}_s$$

where $d_i \in R$ are suitable elements for which $d_s \alpha_{H,s}(c_s) = -\sum_{i \in H^\times} d_i \alpha_{H,i}(c_i)$. □

Theorem 46 (Möller)**.** *[35] With the present notation, denoting*

- $\{A_1, \ldots, A_\mu\}$ *a* $\mathcal{T}^{(m)}$*-homogeneous basis of* $\mathcal{S}_{s-1}$,
- $\mathcal{H}$ *the set of all basic subsets* $H \subset \{1, \ldots, s\} \cap \mathfrak{H}(F)$,
- $\{d_{1H}, \ldots, d_{r_H H}\}$ *a basis of the ideal* $\mathbb{I}_L(\{\alpha_{H,i}(c_i)$ *s.t.* $i \in H^\times\}) : \mathbb{I}_L(\alpha_{H,s}(c_s))$ *for each basic subset* $H \in \mathcal{H}$,
- $D_{jH} \in \mathsf{R}^s$ *a syzygy associated to H and* d_{jH}*, for each basic subset* $H \in \mathcal{H}$ *and each* $j, 1 \leq j \leq r_H$,

the set $\{A_1, \ldots, A_\mu\} \cup \{D_{jH} : H \in \mathcal{H}, 1 \leq j \leq r_H\}$ *is a* $\mathcal{T}^{(m)}$*-homogeneous basis of* $\mathcal{S}_s$.

Proof. Let $S := (d_1\lambda_1, \ldots, d_s\lambda_s) \in \mathcal{S}_s, d_s \neq 0$, be a $\mathcal{T}^{(m)}$-homogeneous element of $\mathcal{T}^{(m)}$-degree $\delta\epsilon$ and let

$$K := \{i, 1 \leq i \leq s : d_i \neq 0\};$$

since by $\mathcal{T}^{(m)}$-homogeneity, $\tau_i \mid \delta$ and $\mathbf{e}_{l_i} = \epsilon$ for each $i \in K$, we have $\mathbf{T}(K) \mid \delta\epsilon$; we also have $d_i = 0$ for each $i \notin K$ and $\lambda_i\tau_i = \delta, \mathbf{e}_{l_i} = \epsilon$ for each $i \in K$.

For the set $H := \{i, 1 \leq i \leq s : \tau_i \mid \tau_K, \mathbf{e}_{l_i} = \varepsilon_K\}$ clearly we have $\tau_H \mid \tau_K$ and $K \subseteq H$ so that $\tau_H \mid \tau_K \mid \delta$; we also have $\varepsilon_H = \varepsilon_K = \epsilon$. Moreover $d_s \neq 0$ implies $s \in K \subseteq H$ so that H is basic. Since $(d_1\lambda_1, \ldots, d_s\lambda_s) \in \mathcal{S}_s$, setting $\upsilon := \frac{\delta}{\tau_H}$, we have

$$0 = \sum_{i=1}^{s} d_i\lambda_i * \mathbf{M}(g_i) = \sum_{i\in H} d_i \frac{\delta}{\tau_i} * c_i\tau_i\epsilon = \left(\sum_{i\in H} d_i\alpha_{\lambda_i}(c_i)\right)\delta\epsilon$$

so that $\sum_{i\in H} d_i\alpha_{\lambda_i}(c_i) = 0$, $\sum_{i\in H} \alpha_\upsilon^{-1}(d_i)\alpha_{H,i}(c_i) = 0$, whence

$$\alpha_\upsilon^{-1}(d_s)\alpha_{H,s}(c_s) \in \mathbb{I}_L(\alpha_{H,i}(c_i) : i \in H^\times) \text{ and } \alpha_\upsilon^{-1}(d_s) \in \mathbb{I}_L(\alpha_{H,i}(c_i) : i \in H^\times) : \mathbb{I}_L(\alpha_{H,s}(c_s)).$$

Therefore, for suitable u_j, $\alpha_\upsilon^{-1}(d_s) = \sum_{j=1}^{r_H} u_j d_{jH}$ and $S - \sum_{j=1}^{r_H} \alpha_\upsilon(u_j)\upsilon * D_{jH} \in \mathcal{S}_{s-1}$. □

Example 47. If we consider the ring of Example 17 as a left $\mathbb{Z}[x]$-module endowed with the Γ-pseudovaluation, $\Gamma = \{Y_1^{a_1}Y_2^{a_2}Y_3^{a_3} : (a_1, a_2, a_1) \in \mathbb{N}^3\}$, we obtain a similar solution as the one described in Example 38 .

Expressing each $\mathbf{M}(f_i)$ as $\mathbf{M}(f_i) = \mathrm{lc}(f_i)\mathbf{T}(f_i)$, according Zacharias approach we need to compute a syzygy bases in $\mathbb{Z}[x]$ among $\alpha_{Y_1}(\mathrm{lc}(f_1)) = (y^2 - 1)$, $\alpha_{Y_2}(\mathrm{lc}(f_2)) = (y^3 - 1)$ and $\alpha_{Y_3}(\mathrm{lc}(f_3)) = (y^4 - 1)$; the natural solutions $(-(y^2 + y + 1), (y + 1), 0)$, $(-(y^2 + 1), 0, 1)$ produce σ_1 and σ_2.

Example 48. In Example 44, the basic elements are the following:

	H	$\mathbf{T}(H)$	f_H
$s = 1$	$\{1\}$	$Y_1Y_2^3Y_3^2$	f_1
$s = 2$	$\{1\}$	$Y_1Y_2^3Y_3^2$	f_1
	$\{2\}$	$Y_1^2Y_2Y_3^2$	f_2
	$\{1, 2\}$	$Y_1^2Y_2^3Y_3^2$	$f_{\{1,2\}} = 4xY_1^2Y_2^3Y_3^2$,
$s = 3$	$\{1\}$	$Y_1Y_2^3Y_3^2$	f_1
	$\{2\}$	$Y_1^2Y_2Y_3^2$	f_2
	$\{3\}$	$Y_1^2Y_2^3Y_3$	f_3
	$\{1, 2, 3\}$	$Y_1^2Y_2^3Y_3^2$	$f_{\{1,2,3\}} = xY_1^2Y_2^3Y_3^2$,
$s = 4$	$\{1\}$	$Y_1Y_2^3Y_3^2$	f_1
	$\{2\}$	$Y_1^2Y_2Y_3^2$	f_2
	$\{3\}$	$Y_1^2Y_2^3Y_3$	f_3
	$\{2, 4\}$	$Y_1^2Y_2^2Y_3^2$	$f_{\{2,4\}} = f_4$
	$\{1, 2, 3, 4\}$	$Y_1^2Y_2^3Y_3^2$	$f_{\{1,2,3,4\}} = f_{\{1,2,3\}}$.

□

Corollary 49. *Assuming that the Zacharias domain R is a principal ideal domain and*

denoting[4]*, for each* $i, j, 1 \leq i < j \leq u$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,

$$\begin{aligned} b(i,j) &:= \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},j}(c_j)} \frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_j} e_j \\ &- \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},i}(c_i)} \frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_i} e_i, \\ B(i,j) &:= \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},j}(c_j)} \frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_j} \star g_j \\ &- \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},i}(c_i)} \frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_i} \star g_i \end{aligned}$$

we have that $\{b(i,j) : 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\}$ *is a left Gebauer–Möller set for* F*, so that* F *is a left Gröbner basis of* M *iff each* $B(i,j)$*,* $1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$*, has a left weak Gröbner representation in terms of* F*.* □

Proof. Since, for any basic subset $H \subset \{1, \ldots, s\} \cap \mathfrak{H}(F)$ we have

$$\begin{aligned} \mathbb{I}(\{\alpha_{\{i,s\},i}(c_i) : i \in H^{\times}\}) : \mathbb{I}(\alpha_{\{i,s\},s}(c_s)) &= \bigoplus (\mathbb{I}(\alpha_{\{i,s\},i}(c_i)) : \mathbb{I}(\alpha_{\{i,s\},s}(c_s))) \\ &= \mathbb{I}\left(\frac{\operatorname{lcm}(\alpha_{\{i,s\},i}(c_i), \alpha_{\{i,s\},s}(c_s))}{\alpha_{\{i,s\},s}(c_s)}\right) \end{aligned}$$

and $b(i,s)$ is the syzygy associated to $\{i,s\}$ and $\frac{\operatorname{lcm}(\alpha_{\{i,s\},i}(c_i), \alpha_{\{i,s\},s}(c_s))}{\alpha_{\{i,s\},s}(c_s)}$. □

Example 50. In Example 44, we obtain the following redundant Gebauer–Möller set (see Example 63)

(i,j)	$\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)$	$\operatorname{lcm}(\tau_i,\tau_j)$	$b(i,j)$			
$(1,2)$	$6^4 \cdot 5x^2$	$Y_1^2Y_2^3Y_3^2$	$(-2^2 3^4 xY_1,$	$5Y_2^2,$	$0,$	$0)$
$(1,3)$	$60x$	$Y_1^2Y_2^3Y_3^2$	$(-3Y_1,$	$0,$	$4Y_3,$	$0)$
$(2,3)$	$6^4 \cdot 5x^2$	$Y_1^2Y_2^3Y_3^2$	$(0,$	$-5Y_2^2,$	$3^3 2^4 xY_3,$	$0)$
$(1,4)$	$60x$	$Y_1^2Y_2^3Y_3^2$	$(-3Y_1,$	$0,$	$0,$	$10Y_2)$
$(2,4)$	6^2x^2	$Y_1^2Y_2^2Y_3^2$	$(0,$	$-Y_2,$	$0,$	$6^2x)$
$(3,4)$	$30x$	$Y_1^2Y_2^3Y_3^2$	$(0,$	$0,$	$-2Y_3,$	$5Y_2)$

□

Corollary 51. *Assuming that the Zacharias domain* R *is a principal ideal domain and that each* α_i *is an automorphism denoting, for each* $i, j, 1 \leq i < j \leq u$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,

$$\begin{aligned} b(i,j) &:= e_j \alpha_{\tau_j}^{-1}\left(\frac{\operatorname{lcm}(c_i,c_j)}{c_j}\right)\frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_j} - e_i \alpha_{\tau_i}^{-1}\left(\frac{\operatorname{lcm}(c_i,c_j)}{c_i}\right)\frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_i} \\ B(i,j) &:= g_j \star \alpha_{\tau_j}^{-1}\left(\frac{\operatorname{lcm}(c_i,c_j)}{c_j}\right)\frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_j} - g_i \star \alpha_{\tau_i}^{-1}\left(\frac{\operatorname{lcm}(c_i,c_j)}{c_i}\right)\frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_i} \end{aligned}$$

[4]Remember that $\alpha_{\{i,j\},j} = \alpha_\tau$ for $\tau = \frac{\operatorname{lcm}(\tau_i,\tau_j)}{\tau_j}$.

we have that $\{b(i,j) : 1 \le i < j \le u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\}$ *is a right Gebauer–Möller set for* F*, so that* F *is a right Gröbner basis of* M *iff each* $B(i,j)$*,* $1 \le i < j \le u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$*, has a right weak Gröbner representation in terms of* F*.* □

6.3 Third algorithm: from weak to strong Gröbner basis

As regards *strong* Gröbner bases, we consider a left Zacharias PID. In this case, we have

Definition 52. A set $C \subset \mathsf{R}^m$ is called a *completion* of F, if, for each subset $H \subset \mathfrak{H}(F)$ which is maximal for $\mathbf{T}(H)$, it contains an element $f_H \in \mathbb{I}(F)$ which satisfies

1. $\mathbf{T}(f_H) = \mathbf{T}(H) = \tau_H \varepsilon_H$,
2. $\mathrm{lc}(f_H) = c_H = \gcd\left(\alpha_{H,i}(\mathrm{lc}(g_i)) : i \in H\right)$,
3. f_H has a left Gröbner representation in terms of F.

Algorithm 53 (Möller)*.* A completion of F can be inductively computed by mimicking the construction of Theorem 46 as follows: the result being trivial if $\#F = 1$, we can assume to have already obtained a completion $C(F^\times)$ of $F^\times = \{g_1, \dots, g_{s-1}\}$, $s \le u$; for each maximal subset $H \subset \{1, \dots, s\}$, if $s \notin H$ we can take as f_H the corresponding element in $C(F^\times)$. If instead $s \in H$, then $H^\times$ is maximal in $F^\times$ for $\mathbf{T}(H^\times)$ and $\tau_{H^\times} \mid \tau_H$; thus there is a corresponding element $f_{H^\times}$ in $C(F^\times)$; let us compute the values $s, t, d \in R$ such that

$$\alpha_{H,H^\times}(\mathrm{lc}(f_{H^\times}))s + \alpha_{H,s}(\mathrm{lc}(g_s))t = \gcd(\alpha_{H,H^\times}(\mathrm{lc}(f_{H^\times})), \alpha_{H,s}(\mathrm{lc}(g_s))) = d$$

and define $f_H := s\frac{\tau_H}{\tau_{H^\times}} \star f_{H^\times} + t\frac{\tau_H}{\tau_s} \star g_s$ which satisfies $\mathbf{M}(f_H) = d\mathbf{T}(H) = d\tau_H\epsilon_H$ so that

1. $\mathbf{T}(f_H) = \mathbf{T}(H) = \tau_H\epsilon_H$,
2. $\mathrm{lc}(f_H) = \gcd(\alpha_{H,H^\times}(\mathrm{lc}(f_{H^\times})), \alpha_{H,s}(\mathrm{lc}(g_s))) = \gcd\left(\alpha_{H,i}(\mathrm{lc}(g_i)) : i \in H\right) = d$,
3. it is sufficient to substitute $f_{H^\times}$ with its left Gröbner representation, to obtain the required Gröbner representation of f_H. □

Proposition 54 (Möller)**.** *With the present notation and under the assumption that* R *is a principal ideal domain, the following conditions are equivalent:*

1. F *is a left Gröbner basis of* M*;*
2. *a completion of* F *is a strong left Gröbner basis of* M*.*

Proof.

(1) $\Longrightarrow$ (2) Let $f \in \mathsf{M}$ and let $f = \sum_{i=1}^{u} h_i \star g_i$ be a left Gröbner representation; denoting $H := \{j : \mathbf{T}(h_j \star g_j) = \mathbf{T}(f) =: \tau\epsilon\}$ we have $\tau_H \mid \tau$, $\epsilon_H = \epsilon$. Thus, setting $\upsilon_j := \frac{\tau}{\tau_j}$, $\omega_j := \frac{\tau_H}{\tau_j}$ for each j and $\lambda := \frac{\tau}{\tau_H}$ we have

$$\begin{aligned}
\mathrm{lc}(f) &= \textstyle\sum_{j\in H} \mathrm{lc}(h_j)\alpha_{\upsilon_j}(\mathrm{lc}(g_j)) \\
&= \textstyle\sum_{j\in H} \mathrm{lc}(h_j)\alpha_\lambda\alpha_{\omega_j}(\mathrm{lc}(g_j)) \quad \in \quad \mathbb{I}\left(\alpha_\lambda\alpha_{\omega_j}(\mathrm{lc}(g_j)) : j \in H\right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad = \quad \alpha_\lambda\left(\mathbb{I}\left(\alpha_{\omega_j}(\mathrm{lc}(g_j)) : j \in H\right)\right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad = \quad \alpha_\lambda(\mathbb{I}(c_H))
\end{aligned}$$

so that $\alpha_\lambda(\mathrm{lc}(f_H)) = \alpha_\lambda(c_H) \mid \mathrm{lc}(f)$ and $\mathrm{lc}(f) = d\alpha_\lambda(\mathrm{lc}(f_H))$ with $d \in R$. In conclusion we have $\mathbf{M}(f) = d\lambda * \mathbf{M}(f_H)$.

(2) $\Longrightarrow$ (1) Let $f \in \mathsf{M}$ and let $f = \sum_{K \subset \mathfrak{H}(F)} c_K \tau_K f_K$ be a strong left Gröbner representation of it in terms of a completion of F; it is sufficient to substitute each f_K with a left Gröbner representation of it in terms of F to obtain the required representation.

□

Example 55. In Example 38, we finally have (see Remark 39)

$$f_{\{1,2\}} = f_{\{1,3\}} = f_{\{1,2,3\}} = \mathfrak{s}_L(\varsigma_A) = \mathfrak{s}_L(\varsigma_B) = (y-1)Y_1^2 Y_2^2 Y_3^2.$$

□

Example 56. In Example 44 the strong Gröbner basis (see Example 48) is

$$\{f_1, f_2, f_3, f_4, f_{\{1,2,3,4\}}\}$$

since

$$\gcd(\alpha_{\{1,2\},\{1\}}(\mathrm{lc}(f_1)), \alpha_{\{1,2\},2}(\mathrm{lc}(f_2))) = \gcd(\alpha_{Y_1}(x), \alpha_{Y_2^2}(x)) = \gcd(20x, 36x) = 4x$$

$$\gcd(\alpha_{\{1,2,3\},\{1,2\}}(\mathrm{lc}(f_{\{1,2\}})), \alpha_{\{1,2,3\},3}(\mathrm{lc}(f_3))) = \gcd(\alpha_1(4x), \alpha_{Y_3}(x)) = \gcd(4x, 15x) = x.$$

Similarly, $f_{\{2,4\}} = f_4$ follows trivially from

$$\gcd(\alpha_{\{2,4\},\{2\}}(\mathrm{lc}(f_2)), \alpha_{\{2,4\},4}(\mathrm{lc}(f_4))) = \gcd(\alpha_{Y_2}(x^2), \alpha_1(x)) = \gcd(36x^2, x) = x.$$

□

6.4 Useless S-pairs and Gebauer-Möller sets

Let us still assume that the Zacharias domain R is a principal ideal domain and we will use freely notations as $\mathbf{M}(i), \mathbf{M}(i,j), \mathbf{M}(i,j,k), 1 \le i,j,k \le u$, instead of $\mathbf{M}(\{i\})$, $\mathbf{M}(\{i,j\})$, $\mathbf{M}(\{i,j,k\})$, introduced in 6.1; we can then easily apply to the present setting the reformulation and improvement by Gebauer–Möller [19] of Buchberger Criteria [9]. However, we must be aware that, in this context, there is no chance of reformulating Buchberger's First Criterion.

Remark 57. In fact, for $F \subset \mathcal{P} = R[Y_1, \ldots, Y_n]$ and $\mathbb{I}(F)$ an ideal of $\mathcal{P}$, we should at least require that

$$\mathbf{M}(i) * \mathbf{M}(j) = \mathbf{M}(j) * \mathbf{M}(i) = \mathbf{M}(i,j)$$

id est not only $\mathrm{lcm}(\tau_i, \tau_j) = \tau_i \circ \tau_j = \tau_j \circ \tau_i$ which is trivially true but also

$$\mathrm{lcm}(\alpha_{\tau_j}(c_i), \alpha_{\tau_i}(c_j)) = c_j \alpha_{\tau_j}(c_i) = c_i \alpha_{\tau_i}(c_j).$$

This essentially requires $c_i \mid \alpha_{\tau_j}(c_i)$ and $c_j \mid \alpha_{\tau_i}(c_j)$ whence $\alpha_{\tau_j} = \mathrm{Id}$; this suggests that Buchberger's First Criterion hardly can be applied.

Note that the proof which considers the trivial sysygies $g_i g_j - g_j g_i = 0$ holds only in the classical polynomial ring case. □

Definition 58. A *useful S-pair set* for F is any subset

$$\mathfrak{GM} \subset \mathcal{S}(u) = \left\{\{i,j\}, 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\right\}$$

such that $\{b(i,j) : \{i,j\} \in \mathfrak{GM}\}$ is a Gebauer–Möller set for F.

Corollary 59. *With the present notation, under the assumption that R is a principal ideal domain, F is a left Gröbner basis of the left module* M *iff, denoting* $\mathfrak{GM}$ *a useful S-pair set for F, each S-polynomial* $B(i,j), \{i,j\} \in \mathfrak{GM}$*, has a left Gröbner representation in terms of F.*

Proof. By definition $\{b(i,j) : \{i,j\} \in \mathfrak{GM}\}$ is a Gebauer–Möller set for F so that, by Theorem 36, F is a Gröbner basis of M iff each S-polynomial $B(i,j), \{i,j\} \in \mathfrak{GM}$, has a Gröbner representation in terms of F. □

If we moreover define,

- for each $i,j : 1 \leq i,j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,
  - $c(i,j) = \operatorname{lcm}(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j))$,
  - $\tau(i,j) = \operatorname{lcm}(\tau_i, \tau_j)$,
  - $\mu(i,j) = c(i,j)\tau(i,j)$,
- and for each $i,j,k : 1 \leq i,j,k \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j} = \mathbf{e}_{l_k}$,
  - $c(i,j,k) = \operatorname{lcm}(\alpha_{\{i,j,k\},\{i,j\}}(c(i,j)), \alpha_{\{i,j,k\},\{i,k\}}(c(i,k)), \alpha_{\{i,j,k\};\{j,k\}}(c(j,k)))$,
  - $\tau(i,j,k) = \operatorname{lcm}(\tau_i, \tau_j, \tau_k)$,
  - $\mu(i,j,k) = c(i,j,k)\tau(i,j,k)$

  and we impose on the set

$$\mathcal{S}(u) := \left\{\{i,j\}, 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\right\}$$

the ordering $\prec$ defined by

$$\{i_1,j_1\} \prec \{i_2,j_2\} \iff \begin{cases} \tau(i_1,j_1) < \tau(i_2,j_2) & \text{or} \\ \tau(i_1,j_1) = \tau(i_2,j_2), j_1 < j_2 & \text{or} \\ \tau(i_1,j_1) = \tau(i_2,j_2), j_1 = j_2, i_1 < i_2, & \end{cases} \tag{8}$$

we obtain

Definition 60. An S-element $b(i,j), 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$, and the related S-pair $\{i,j\}$ are called *redundant* if either

(a). exists $k > j, \mathbf{e}_{l_k} = \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$ such that

$$\mu(i,j,k) = \mu(i,j);\ \mu(i,k) \neq \mu(i,j) \neq \mu(j,k)$$

(b). or exists $k < j, \mathbf{e}_{l_k} = \mathbf{e}_{l_i} = \mathbf{e}_{l_j} : \mu(k,j) \mid \mu(i,j) \neq \mu(k,j)$. □

Lemma 61 (Möller)**.** *The following holds*

1. *for each* $i, j, k : 1 \le i, j, k \le u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j} = \mathbf{e}_{l_k}$, *it holds*

$$\frac{\mu(i,j,k)}{\mu(i,k)} b(i,k) - \frac{\mu(i,j,k)}{\mu(i,j)} b(i,j) + \frac{\mu(i,j,k)}{\mu(k,j)} b(k,j) = 0.$$

2. $\mathfrak{R} := \{b(i,j), 1 \le i < j \le u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$ *and not redundant*$\}$ *is a useful S-element set.*

3. *Let* $G := \{g_1, \ldots, g_s\}, s \le u$, *and let*

$$\mathfrak{GM}_* \subset \{\{i,j\}, 1 \le i < j < s, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\}$$

be a useful S-pair set for $G_* = \{g_1, \ldots, g_{s-1}\}$.
Let $\overline{M} := \{\mu(j,s) : 1 \le j < s, \mathbf{e}_{l_j} = \mathbf{e}_{l_s}\}$ *and let* $\overline{M}' \subset \overline{M}$ *be the set of the elements* $\mu := \mu(j,s) \in \overline{M}$ *such that there exists* $\mu(j',s) \in \overline{M} : \mu(j',s) \mid \mu(j,s) \ne \mu(j',s)$.
For each $\mu := \mathbf{M}(j,s) \in \overline{M} \setminus \overline{M}'$ *let* $i_\mu, 1 \le i_\mu < s$, *be such that* $\mu = \mathbf{M}(i_\mu, s)$. *Then*

$$\mathfrak{GM} := \mathfrak{GM}_* \cup \{\{i_\mu, s\} : \mu \in \overline{M} \setminus \overline{M}'\}$$

is a useful S-pair set for G.

Proof. 1. (*cf.* [31, Lemma 25.1.4]) One has

$$\begin{aligned}
& \frac{\mu(i,j,k)}{\mu(i,k)} * b(i,k) - \frac{\mu(i,j,k)}{\mu(i,j)} * b(i,j) + \frac{\mu(i,j,k)}{\mu(k,j)} * b(k,j) \\
= \; & \frac{\mu(i,j,k)}{\mu(i,k)} * \left(\frac{\mu(i,k)}{\mu(k)} e_k - \frac{\mu(i,k)}{\mu(i)} e_i \right) \\
- \; & \frac{\mu(i,j,k)}{\mu(i,j)} * \left(\frac{\mu(i,j)}{\mu(j)} e_j - \frac{\mu(i,j)}{\mu(i)} e_i \right) \\
+ \; & \frac{\mu(i,j,k)}{\mu(k,j)} * \left(\frac{\mu(k,j)}{\mu(j)} e_j - \frac{\mu(k,j)}{\mu(k)} e_k \right) \\
= \; & \left(\frac{\mu(i,j,k)}{\mu(k)} e_k - \frac{\mu(i,j,k)}{\mu(i)} e_i \right) \\
- \; & \left(\frac{\mu(i,j,k)}{\mu(j)} e_j - \frac{\mu(i,j,k)}{\mu(i)} e_i \right) \\
+ \; & \left(\frac{\mu(i,j,k)}{\mu(j)} e_j - \frac{\mu(i,j,k)}{\mu(k)} e_k \right) \\
= \; & 0
\end{aligned}$$

2. (*cf.* [31, Lemma 25.1.8]) In order to prove the claim by induction, it is sufficient to show that, for each redundant $\{i,j\}, 1 \le i < j \le u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j} =: \epsilon$, there are
   - $\{i_1, j_1\}, \ldots, \{i_\rho, j_\rho\}, \ldots, \{i_r, j_r\}, 1 \le i_\rho < j_\rho \le u, \mathbf{e}_{l_{i_\rho}} = \mathbf{e}_{l_{j_\rho}} = \epsilon$,
   - elements $t_1, \ldots, t_r \in \mathcal{T}$,

– and coefficients $c_1, \dots c_r \in R \setminus \{0\}$

such that

– $b(i,j) = \sum_\rho c_\rho t_\rho * b(i_\rho, j_\rho)$;
– $\tau(i,j) = t_\rho \circ \tau(i_\rho, j_\rho)$, for each ρ;
– $\{i_\rho, j_\rho\} \prec \{i,j\}$.

In order to show this, we only need to consider the representation

$$b(i,j) = \frac{\mu(i,j,k)}{\mu(i,k)} * b(i,k) + \frac{\mu(i,j,k)}{\mu(k,j)} * b(k,j)$$

and to prove that

$$\{i,k\} \prec \{i,j\} \succ \{k,j\};$$

this happens (according to the two cases of the definition) because

(a) $\tau(i,k) \mid \tau(i,j,k) = \tau(i,j) \neq \tau(i,k)$ implies $\{i,k\} \prec \{i,j\}$ and the same argument proves $\{j,k\} \prec \{i,j\}$;
(b) the same argument as that above proves $\{j,k\} \prec \{i,j\}$, while $\{i,k\} \prec \{i,j\}$ because $\tau(i,k) \leq \tau(i,j)$ and $k < j$.

3. (*cf.* [31, Lemma 25.1.9]) Let $i < s, \mathbf{e}_{l_i} = \mathbf{e}_{l_s} =: \epsilon, \mu := \mu(i,s)$. Then:

– if there exists $\mu' \in \overline{M}$ such that $\mu(i_{\mu'}, s) = \mu' \mid \mu(i,s) \neq \mu'$, then since $i_{\mu'} < s$, $\{i,s\}$ is redundant;
– if $i = i_\mu$ then $\{i_m, s\} \in \mathfrak{GM}$;
– if $i \neq i_\mu$ then $b(i,s) = \frac{\mu(i,i_\mu,s)}{\mu(i,i_\mu)} b(i,i_\mu) - b(i_\mu, s)$.

□

Corollary 62. *With the present notation, under the assumption that R is a principal ideal domain, F is a left Gröbner basis of* M *iff each S-polynomial B(i, j), with* $b(i,j) \in \mathfrak{R}$*, has a left Gröbner representation in terms of F.* □

Example 63. In connection with Lemma 61 we have

(i,j,k)	$c(i,j,k)$	$\mu(i,j,k)$	$b(i,j,k)$
$(1,2,3)$	$6^4 \cdot 5x^2$	$Y_1^2 Y_2^3 Y_3^2$	$b(1,2) - 2^2 3^3 x b(1,3) + b(2,3) = 0,$
$(1,2,4)$	$6^4 \cdot 5x^2$	$Y_1^2 Y_2^3 Y_3^2$	$b(1,2) - 2^2 3^3 x b(1,4) + 5Y_2 * b(2,4) = 0,$.
$(1,3,4)$	$60x$	$Y_1^2 Y_2^3 Y_3^2$	$b(1,3) - b(1,4) + 2b(3,4) = 0.$
$(2,3,4)$	$6^4 \cdot 5x^2$	$Y_1^2 Y_2^3 Y_3^2$	$b(2,3) - 5Y_2 * b(2,4) + 6^3 b(3,4) = 0.$

Note that we obviously [20, 34] have also

$$b(1,2,3) - b(1,2,4) + 2^2 3^3 x b(1,3,4) - b(2,3,4).$$

Thus the redundant elements are $b(2,3)$ via 1 or 4, $b(1,2)$ via 4 and $b(1,4)$ via 3.

But, as it is well-known, it is more efficient (at least for storing considerations) the algorithm sketched in Lemma 61.3 which

for $s = 2$ stores $(1, 2)$,

for $s = 3$ stores $(1, 3)$,

for $s = 4$ removes $(1, 2)$ and stores $(2, 4)$ and $(3, 4)$.

Thus the Gebauer-Möller set is still

$$\{b(1,3), b(2,4), b(3,4)\}$$

while

$$\begin{aligned} b(1,4) &= b(1,3) + 2b(3,4), \\ b(2,3) &= 5Y_2 * b(2,4) + 6^3 b(3,4), \\ b(1,2) &= 2^2 3^3 x b(1,4) - 5Y_2 * b(2,4). \end{aligned}$$

□

7 Weispfenning Completions for Bilateral Gröbner basis for Multivariate Ore Extensions of Zacharias Domains

7.1 Kandri-Rody–Weispfenning completion

Let R be a not necessarily commutative domain and R a multivariate Ore extension.

The most efficient technique for producing bilateral Gröbner bases $G := \mathbb{I}_2(F)$ in a noetherian Ore extension is Kandri-Rody–Weispfenning completion [22]. Iteratively:

- Repeat
  - Compute a left-Gröbner basis G of the ideal $\mathbb{I}_L(F)$;
  - for each $g \in G, 1 \leq i \leq n$, compute the normal form $\mathrm{NF}(g \star Y_i, \mathbb{I}_L(F))$ of $g \star Y_i$ w.r.t. G;
  - set $H := \{\mathrm{NF}(g \star Y_i, \mathbb{I}_L(F)), g \in G, 1 \leq i \leq n\}$, $F := G \cup H$

  until $H = \{0\}$.

The *rationale* of the algorithm is

Lemma 64 (Kandri-Rody–Weispfenning)**.** *For $G \subset \mathsf{R}$ the following conditions are equivalent:*

1. $\mathbb{I}_L(G) = \mathbb{I}_2(G)$*;*
2. *for each $\tau \in \mathcal{T}$ and each $g \in G$, $g \star \tau \in \mathbb{I}_L(G)$;*
3. *for each $i, 1 \leq i \leq n$, and each $g \in G$, $g \star Y_i \in \mathbb{I}_L(G)$.*

Proof.

(1) $\implies$ (2) $\iff$ (3) is trivial.

(2) $\implies$ (1) $\mathcal{B}_2(G) := \{\lambda \star g \star \rho : \lambda, \rho \in \mathcal{T}, g \in G\}$ is an R-linear basis of $\mathbb{I}_2(G)$ and satisfies

$$\mathcal{B}_2(G) = \{\lambda \star (g \star \rho) : \lambda, \rho \in \mathcal{T}, g \in G\} \subseteq \{\lambda \star h : \lambda \in \mathcal{T}, h \in \mathbb{I}_L(G)\} \subseteq \mathbb{I}_L(G).$$

□

7.2 Weispfenning: Restricted Representation and Completion

We remark that a generic ring R can be effectively given as a quotient of a free monoid ring $\mathcal{R} := \mathbb{Z}\langle\overline{\mathbf{v}}\rangle$ over $\mathbb{Z}$ and the monoid $\langle\overline{\mathbf{v}}\rangle$ of all words over the alphabet $\overline{\mathbf{v}}$ modulo a bilateral ideal I, so, in this section, $R = \mathcal{R}/\mathsf{I}$.

We must restrict ourselves to the case in which $<$ is a sequential term-ordering, *id est* for each $\tau \in \mathcal{T}$, the set $\{\omega \in \mathcal{T} : \omega < \tau\}$ is finite.

Lemma 65. *[53] Let*

$$F := \{g_1, \ldots, g_u\} \subset \mathsf{R}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i\tau_i\mathbf{e}_{l_i} - p_i;$$

set $\Omega := \max_<\{\mathbf{T}(g_i) : 1 \leq i \leq u\}$.

Let M *be the bilateral module* $\mathsf{M} := \mathbb{I}_2(F)$ *and* $\mathbb{I}_W(F)$ *the restricted module*

$$\mathbb{I}_W(F) := \mathrm{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{T}, f \in F).$$

If every $f \star \alpha_\upsilon(v), f \in F, v \in \overline{\mathbf{v}}, \upsilon \in \mathcal{T}, \upsilon < \Omega$*, has a restricted representation in terms of* F *w.r.t. a sequential term-ordering* $<$*, then every* $f \star r, f \in F, r \in \mathsf{R}$*, has a restricted representation in terms of* F *w.r.t.* $<$*.*

Proof. We can wlog assume $r = \prod_{i=1}^{\nu} v_i, v_i \in \overline{\mathbf{v}}$ and prove the claim by induction on $\nu \in \mathbb{N}$.

Thus we have a restricted representation in terms of F

$$f \star \left(\prod_{i=1}^{\nu-1} v_i\right) = \sum_j d_j g_{i_j} \star \rho_j, \tau_{i_j} \circ \rho_j \leq \mathbf{T}(f),$$

whence we obtain

$$f \star \prod_{i=1}^{\nu} v_i = f \star \prod_{i=1}^{\nu-1} v_i \star v_\nu = \sum_j d_j g_{i_j} \star \rho_j \star v_\nu = \sum_j d_j g_{i_j} \star \alpha_{\rho_j}(v_\nu)\rho_j$$

and since $\rho_j < \mathbf{T}(f) \leq \Omega$ each element $g_{i_j} \star \alpha_{\rho_j}(v_\nu)$ can be substituted with its restricted representation whose existence is granted by assumption. □

Lemma 66. *[53] Under the same assumption, if, for each* $g_j \in F$*, both* $Y_i \star g_j, 1 \leq i \leq n$*, and each* $g_j \star \alpha_\upsilon(v), v \in \overline{\mathbf{v}}, \upsilon \in \mathcal{T}, \upsilon < \Omega$*, have a restricted representation in terms of* F *w.r.t.* $<$*, then* $\mathbb{I}_W(F) = \mathsf{M}$*.*

Proof. It is sufficient to show that, for each $f \in \mathbb{I}_W(F)$, both each $Y_i \star f \in \mathbb{I}_W(F), 1 \leq i \leq n$, and each $f \star v \in \mathbb{I}_W(F), v \in \overline{\mathbf{v}}$.

By assumption $f = \sum_j d_j g_{i_j} \star \rho_j, d_j \in R \setminus \{0\}, \rho_j \in \mathcal{T}, 1 \leq i_j \leq u$, so that

$$Y_i \star f = \sum_j \alpha_i(d_j) \star (Y_i \star g_{i_j}) \star \rho_j \text{ and } f \star v = \sum_j d_j(g_{i_j} \star \alpha_{\rho_j}(v)) \star \rho_j;$$

by assumption each $Y_i \star g_{i_j}$ has a restricted representation in terms of F; for the Lemma above, also each $g_{i_j} \star \alpha_{\rho_j}(v)$ has a restricted representation in terms of F. □

Corollary 67. *[53] Let*

$$F := \{g_1, \ldots, g_u\} \subset \mathsf{R}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{l_i} - p_i.$$

Let M *be the bilateral module* $\mathsf{M} := \mathbb{I}_2(F)$ *and* $\mathbb{I}_W(F)$ *the restricted module*

$$\mathbb{I}_W(F) := \mathrm{Span}_R(af \star \rho : a \in R \setminus \{0\}, \rho \in \mathcal{T}, f \in F).$$

F is the bilateral Gröbner basis of M *iff*

1. *denoting $\mathfrak{GM}(F)$ any restricted Gebauer–Möller set for F, each $\sigma \in \mathfrak{GM}(F)$ has a restricted quasi-Gröbner representation in terms of F;*
2. *for each $g_j \in F$, both $Y_i \star g_j, 1 \leq i \leq n$ and each $g_j \star \alpha_v(v), v \in \overline{\mathbf{v}}, v \in \mathcal{T}, v < \Omega$, have a restricted representation in terms of F w.r.t. $<$.*

7.3 Gebauer-Möller sets for Restricted Gröbner bases

In this section we assume, as in section 6.4, that the Zacharias domain R is a principal ideal domain; R is intended to be a multivariate Ore extension.

It is clear from Corollary 67 that the computation of a Gröbner basis can be obtained via Weispfenning's completion, provided that we are able to produce restricted Gebauer-Möller sets; to do so, we need only to properly reformulate the results of Section 6.4.

We begin by remarking [12] that for each monomial $c\tau \in \mathsf{M}(\mathsf{R})$ the function $g \mapsto cg \star \tau$ distributes, thus we can define a multiplication $\diamond : \mathsf{R} \times \mathsf{R} \to \mathsf{R}$ by setting

$$c_i\tau_i \diamond c_j\tau_j := c_i c_j \tau_j \tau_i = c_j c_i \tau_i \tau_j =: c_j\tau_j \diamond c_i\tau_i$$

which of course is commutative and thus, granting the trivial syzygy

$$g_i \diamond g_j = g_j \diamond g_i$$

allows to recover Buchberger First Criterion.

As a consequence, we can reformulate the notion of restricted Gröbner representation:

– we say that $f \in \mathsf{R}^m \setminus \{0\}$ has a restricted *Gröbner representation* in terms of G if it can be written as $f = \sum_{i=1}^u l_i \diamond g_i$, with $l_i \in \mathsf{R}, g_i \in G$ and $\mathbf{T}(l_i) \circ \mathbf{T}(g_i) \leq \mathbf{T}(f)$ for each i.

Let us denote, for each $i, j, 1 \leq i < j \leq u$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,

$$\begin{aligned} b_W(i,j) &:= \frac{\mathrm{lcm}(c_i,c_j)}{c_j} e_j \frac{\mathrm{lcm}(\tau_i,\tau_j)}{\tau_j} - \frac{\mathrm{lcm}(c_i,c_j)}{c_i} e_i \frac{\mathrm{lcm}(\tau_i,\tau_j)}{\tau_i} \\ &= \frac{\mathbf{M}(i,j)}{\mathbf{M}(j)} \diamond e_j - \frac{\mathbf{M}(i,j)}{\mathbf{M}(i)} \diamond e_i \in \ker(\mathfrak{s}_W), \\ B_W(i,j) &:= \frac{\mathrm{lcm}(c_i,c_j)}{c_j} g_j \star \frac{\mathrm{lcm}(\tau_i,\tau_j)}{\tau_j} - \frac{\mathrm{lcm}(c_i,c_j)}{c_i} g_i \star \frac{\mathrm{lcm}(\tau_i,\tau_j)}{\tau_i} \\ &= \frac{\mathbf{M}(i,j)}{\mathbf{M}(j)} \diamond g_j - \frac{\mathbf{M}(i,j)}{\mathbf{M}(i)} \diamond g_i \end{aligned}$$

and let us explicitly assume that

– for each $g_j \in F$, both $Y_i \star g_j, 1 \leq i \leq n$, and each $g_j \star \alpha_\upsilon(v), v \in \overline{\mathbf{v}}, \upsilon \in \mathcal{T}, \upsilon < \Omega$, have a restricted representation in terms of F w.r.t. $<$.

Lemma 68 (Buchberger's First Criterion)**.** *If $m = 1$,* id est *$F \subset \mathsf{R}$ and $\mathbb{I}_W(F)$ is an ideal of R, then*

$$\begin{aligned} \mathbf{M}(i) \diamond \mathbf{M}(j) = \mathbf{M}(i,j) \quad &\Longleftrightarrow \quad \mathrm{lcm}(\tau_i,\tau_j) = \tau_i\tau_j \text{ and } \mathrm{lcm}(c_i,c_j) = c_ic_j \\ &\Longrightarrow \quad \mathrm{NF}_W(B_W(i,j),F) = 0. \end{aligned}$$

Proof. We will prove that $B_W(i,j)$ has a restricted Gröbner representation in terms of F; thus the result will follow by the equivalence (4) $\Longleftrightarrow$ (8) in Proposition 19.

Remark that

$$p_i := g_i - \mathbf{M}(i) = \sum_l c_{il}t_{il} \text{ and } p_j := g_j - \mathbf{M}(j) = \sum_k c_{jk}t_{jk}$$

satisfy $\mathbf{T}(p_i) < \mathbf{T}(g_i)$, $\mathbf{T}(p_j) < \mathbf{T}(g_j)$.

Then it holds:

$$0 = g_i \diamond g_j - g_j \diamond g_i = \mathbf{M}(i) \diamond g_j + p_i \diamond g_j - \mathbf{M}(j) \diamond g_i - p_j \diamond g_i,$$

and

$$B_W(i,j) := \frac{\mathbf{M}(i,j)}{\mathbf{M}(j)} \diamond g_j - \frac{\mathbf{M}(i,j)}{\mathbf{M}(i)} \diamond g_i = \mathbf{M}(i) \diamond g_j - \mathbf{M}(j) \diamond g_i = p_j \diamond g_i - p_i \diamond g_j.$$

There are then two possibilities: either

– $\mathbf{M}(p_j) \diamond \mathbf{M}(g_i) \neq \mathbf{M}(p_i) \diamond \mathbf{M}(g_j)$ in which case

$$\mathbf{T}(B_W(i,j)) = \max(\mathbf{T}(p_j) \circ \mathbf{T}(g_i), \mathbf{T}(p_i) \circ \mathbf{T}(g_j))$$

and

$$B_W(i,j) = p_j \diamond g_i - p_i \diamond g_j = \sum_k c_{jk} g_i \star t_{jk} - \sum_l c_{il} g_j \star t_{il}$$

is a restricted Gröbner representation;

– or $\mathbf{M}(p_j) \diamond \mathbf{M}(g_i) = \mathbf{M}(p_i) \diamond \mathbf{M}(g_j)$, $\mathbf{T}(B_W(i,j)) < \mathbf{T}(p_j) \circ \mathbf{T}(g_i) = \mathbf{T}(p_i) \circ \mathbf{T}(g_j)$, in which case $B_W(i,j) = p_j \diamond g_i - p_i \diamond g_j$ would not be a Gröbner representation.

But the latter case is impossible: in fact, from

$$\operatorname{lcm}(\mathbf{T}(g_i), \mathbf{T}(g_j)) \mid \mathbf{T}(p_i) \circ \mathbf{T}(g_j) = \mathbf{T}(p_j) \circ \mathbf{T}(g_i) < \mathbf{T}(g_j) \circ \mathbf{T}(g_i)$$

we deduce $\operatorname{lcm}(\mathbf{T}(g_i), \mathbf{T}(g_j)) \neq \mathbf{T}(g_j) \circ \mathbf{T}(g_i)$ and $\mathbf{T}(i,j) \neq \mathbf{T}(i) \circ \mathbf{T}(j)$ contradicting the assumption $\mathbf{M}(i,j) = \mathbf{M}(i) \diamond \mathbf{M}(j)$. □

Definition 69. Denote

$$\mathfrak{C}_u := \begin{cases} \left\{ \{i,j\} : \mathbf{M}(i) \diamond \mathbf{M}(j) = \mathbf{M}(i,j) \right\} & \text{if } \mathsf{M} \text{ is an ideal} \\ \emptyset & \text{otherwise.} \end{cases}$$

A *useful S-pair set* for F is any subset

$$\mathfrak{GM} \subset \mathcal{S}(u) = \left\{ \{i,j\}, 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j} \right\}$$

such that $\{b(i,j) : \{i,j\} \in \mathfrak{GM} \cup \mathfrak{C}_u\}$ is a Gebauer–Möller set for F.

Corollary 70. *With the present notation, under the assumption that R is a principal ideal domain, F is a Gröbner basis of M iff, denoting $\mathfrak{GM}$ a useful S-pair set for F, each S-polynomial $B_W(i,j), \{i,j\} \in \mathfrak{GM}$, has a Gröbner representation in terms of F.*

Proof. By definition $\{b_W(i,j) : \{i,j\} \in \mathfrak{GM} \cup \mathfrak{C}_u\}$ is a Gebauer–Möller set for F so that, by Theorem 36, F is a Gröbner basis of M iff each S-polynomial $B_W(i,j), \{i,j\} \in \mathfrak{GM} \cup \mathfrak{C}_u$ has a Gröbner representation in terms of F.

The claim is a direct consequence of Buchberger's First Criterion which states that for each $\{i,j\} \in \mathfrak{C}_u$, $B_W(i,j)$ has a weak Gröbner representation in terms of F. □

Definition 71. An S-element $b(i,j), 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$, and the related S-pair $\{i,j\}$ are called *redundant* if either

(a). exists $k > j$, $\mathbf{e}_{l_k} = \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$ such that

$$\mathbf{M}(i,j,k) = \mathbf{M}(i,j);\ \mathbf{M}(i,k) \neq \mathbf{M}(i,j) \neq \mathbf{M}(j,k),$$

(b). or exists $k < j, \mathbf{e}_{l_k} = \mathbf{e}_{l_i} = \mathbf{e}_{l_j} : \mathbf{M}(j,k) \mid \mathbf{M}(i,j) \neq \mathbf{M}(j,k)$. □

Lemma 72 (Möller)**.** *The following holds*

1. *for each $i,j,k : 1 \leq i,j,k \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j} = \mathbf{e}_{l_k}$, it holds*

$$\frac{c(i,j,k)}{c(i,k)} b(i,k) * \frac{\tau(i,j,k)}{\tau(i,k)} - \frac{c(i,j,k)}{c(i,j)} b(i,j) * \frac{\tau(i,j,k)}{\tau(i,j)} + \frac{c(i,j,k)}{c(k,j)} b(k,j) * \frac{\tau(i,j,k)}{\tau(k,j)} = 0.$$

2. *$\mathfrak{R} := \{b(i,j), 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$ and not redundant$\}$ is a useful S-element set.*

3. *Let* $G := \{g_1, \ldots, g_s\}$, $s \leq u$, *and let*

$$\mathfrak{GM}_* \subset \{\{i, j\}, 1 \leq i < j < s, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\}$$

be a useful S-pair set for $G_* = \{g_1, \ldots, g_{s-1}\}$.
Let $\overline{M} := \{\mathbf{M}(j, s) : 1 \leq j < s, \mathbf{e}_{l_j} = \mathbf{e}_{l_s}\}$ *and let* $\overline{M}' \subset \overline{M}$ *be the set of the elements* $\mu := \mathbf{M}(j, s) \in \overline{M}$ *such that either*

- *there exists* $\mathbf{M}(j', s) \in \overline{M} : \mathbf{M}(j', s) \mid \mathbf{M}(j, s) \neq \mathbf{M}(j', s)$ *or*
- *(in case* M *is an ideal) there exists* $i_\mu, 1 \leq i_\mu < s$:

$$\mathbf{M}(i_\mu) \diamond \mathbf{M}(s) = \mathbf{M}(i_\mu, s) = \mu.$$

For each $\mu := \mathbf{M}(j, s) \in \overline{M} \setminus \overline{M}'$ *let* $i_\mu, 1 \leq i_\mu < s$, *be such that* $\mu = \mathbf{M}(i_\mu, s)$. *Then*

$$\mathfrak{GM} := \mathfrak{GM}_* \cup \{\{i_\mu, s\} : \mu \in \overline{M} \setminus \overline{M}'\}$$

is a useful S-pair set for G.

Proof. The proof is an adaptation of the one given in Lemma 61. □

Corollary 73. *With the present notation, under the assumption that R is a principal ideal domain, F is a restricted Gröbner basis of* M *iff*

1. *each S-polynomial* $B_W(i, j), \{i, j\} \in \mathfrak{R}$, *has a restricted Gröbner representation in terms of F;*
2. *for each* $g_j \in F$, *both* $Y_i \star g_j, 1 \leq i \leq n$ *and each* $g_j \star \alpha_\upsilon(v), v \in \overline{\mathbf{v}}, \upsilon \in \mathcal{T}, \upsilon < \Omega$, *have a restricted representation in terms of F w.r.t.* $<$.

□

8 Structural Theorem for Multivariate Ore Extensions of Zacharias PIDs

Theorem 74 (Structural Theorem)**.** *Let R be a left Zacharias principal ideal domain,* $\mathsf{R} := R[Y_1, \ldots, Y_n]$ *a multivariate Ore extension of R,* $<$ *a term-ordering,* $\mathsf{M} \subset \mathsf{R}^m$ *a left module generated by a basis* $F := \{g_1, \ldots, g_u\} \subset \mathsf{M}$, $\mathbf{M}(g_i) = c_i \tau_i \mathbf{e}_{l_i}$, $C(F)$ *a completion of F,* $\mathfrak{R} := \{B(i, j), 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$ *and not redundant*$\}$.
Then the following conditions are equivalent:

(1). *F is a left Gröbner basis of* M*;*

(1_s). *C(F) is a left strong Gröbner basis of* M*;*

(2). $\mathcal{B}(F) := \{\lambda g : \lambda \in \mathcal{T}, g \in F\}$ *is a Gauss generating set* [31, Definition 21.2.1]*;*

(3). $f \in \mathsf{M} \iff$ *it has a left Gröbner representation in terms of F;*

(4). $f \in \mathsf{M} \iff$ *it has a left strong Gröbner representation in terms of* $C(F)$*;*

(5). *for each* $f \in \mathsf{R}^m \setminus \{0\}$ *and any normal form* h *of* f *w.r.t.* F*, we have*

$$f \in \mathsf{M} \iff h = 0;$$

(5_s). *for each* $f \in \mathsf{R}^m \setminus \{0\}$ *and any strong normal form* h *of* f *w.r.t.* $C(F)$*, we have*

$$f \in \mathsf{M} \iff h = 0;$$

(6). *for each* $f \in \mathsf{R}^m \setminus \{0\}$, $f - \mathrm{Can}(f, \mathsf{M})$ *has a strong Gröbner representation in terms of* $C(F)$*;*

(7). *each* $B(i, j) \in \Re$ *has a weak Gröbner representation in terms of* F*;*

(8). *for each element* σ *of a Gebauer–Möller set for* F*, the S-polynomial* $\Im_L(\sigma)$ *has a left quasi-Gröbner representation in terms of* F*.*

Proof.

(1) $\iff$ (1_s) is Proposition 54;

(1) $\iff$ (2) is trivial;

(1) $\iff$ (5) $\iff$ (3) is Proposition 19;

(1_s) $\iff$ (4) $\iff$ (5_s) is Proposition 19;

(1) $\implies$ (6) is the content of Section 6.3;

(6) $\implies$ (4) because for each $f \in \mathsf{M}, \mathrm{Can}(f, \mathsf{M}) = 0$;

(1) $\iff$ (7) is Corollary 49;

(1) $\iff$ (3) $\iff$ (8) is Theorem 36.

□

9 Spear's Theorem

For Gröbner bases in a ring $\mathcal{A}$ given as quotient

$$\Pi : Q := \mathbb{Z}\langle Z_1, \ldots, Z_n\rangle \twoheadrightarrow \mathcal{A} \cong Q/\mathcal{I}, \quad \mathcal{I} := \ker(\Pi),$$

of a free assocative algebra, a general approach is to directly apply Spear's Theorem [49] [31, Proposition 24.7.3] [29], which, though not a tool for computation, can be helpful in order to understand the structure of $\mathcal{A}$.

For the present setting, denoting

- $f_{ij} := Y_j Y_i - \alpha_j(Y_i) Y_j - \delta_j(Y_i), 1 \le i < j \le n$,
- $C := \{f_{ij} : 1 \le i < j \le n\}$,

– $\mathcal{I} := \mathbb{I}_2(C)$

and for each $m \in \mathbb{N}$,

– $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ the canonical basis of R^m,

– $C^{(m)} := \{f_{ij\iota} := f_{ij}\mathbf{e}_\iota : 1 \leq i < j \leq n, 1 \leq \iota \leq m\}$,

we have the presentation

$$\mathsf{R} = Q/\mathcal{I}, \mathcal{I} := \ker(\Pi), \Pi : Q := R\langle Y_1, \ldots, Y_n\rangle \twoheadrightarrow \mathsf{R}$$

and, for each free R-module $\mathsf{R}^m, m \in \mathbb{N}$, the projection Π extends to the canonical projections, still denoted Π,

$$\Pi : Q^m \twoheadrightarrow \mathsf{R}^m, \ker(\Pi) = \mathcal{I}^m = \mathbb{I}_2(C^{(m)}).$$

Thus denoting

– $F := \{g_1, \ldots, g_u\} \subset \mathsf{R}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i\tau_i\mathbf{e}_{l_i} - p_i$,

– $\mathsf{M} \subset \mathsf{R}^m$ the module $\mathsf{M} := \mathbb{I}_2(F)$,

– $\mathsf{M}' := \Pi^{-1}(\mathsf{M}) = \mathsf{M} + \mathcal{I}^m \subset Q^m$,

we can reformulate Spear's result as

Lemma 75. *[29, Lemma 12] Assume $F \subset \mathsf{M}'$ is a Gröbner basis of M' and denote*

$$\bar{F} := \{\mathrm{Can}(g, \mathcal{I}^m) : g \in F, \mathbf{T}(g) \notin \mathbf{T}(\mathcal{I}^{(m)})\} \subset R[Y_1, \ldots, Y_n]^m$$

where $\mathrm{Can}(g, \mathcal{I}^m)$ denotes the canonical form of $g \in Q^m$ w.r.t. $C^{(m)}$ so that in particular $g = \Pi(g)$ for each $g \in \bar{F}$.

Then $\bar{F} \sqcup C^{(m)}$ is a Gröbner basis of M'.

Theorem 76 (Spear)**.** *[29, Theorem 13] With the present notation, the following holds:*

1. *if F is a reduced Gröbner basis of M', then*

$$\begin{aligned}\{g \in F : g = \Pi(g)\} &= \{\Pi(g) : g \in F, \mathbf{T}(g) \notin \mathbf{T}(\mathcal{I}^{(m)})\} \\ &= F \cap R[Y_1, \ldots, Y_n]^m\end{aligned}$$

   is a reduced Gröbner basis of M;

2. *if $F \subset R[Y_1, \ldots, Y_n]^m$, so that in particular $\Pi(f) = f$ for each $f \in F$, is the Gröbner basis of M, then $F \sqcup C^{(m)}$ is a Gröbner basis of M'.*

3. *Assume each $m' \in \mathsf{M}'$ has a Gröbner representation in terms of $F \subset \mathsf{M}'$.*

   Set

$$\bar{F} := \{\mathrm{Can}(g, \mathcal{I}^m) : g \in F, g \notin \mathcal{I}^m\} \subset R[Y_1, \ldots, Y_n]^m$$

   where $\mathrm{Can}(g, \mathcal{I}^m) \in R[Y_1, \ldots, Y_n]^m$ denotes the canonical form of $g \in Q^m$ w.r.t. $C^{(m)}$ so that in particular $g = \Pi(g)$ for each $g \in \bar{F}$.

   Then each $m \in \mathsf{M}$ has a Gröbner representation in terms of $\bar{F}$.

4. *if $F \subset R[Y_1, \ldots, Y_n]^m$, so that in particular $\Pi(f) = f$ for each $f \in F$, is such that each $m \in \mathsf{M}$ has a Gröbner representation in terms of F, then each $m' \in \mathsf{M}'$ has a Gröbner representation in terms of $F \sqcup C^{(m)}$.*

Corollary 77. *[29, Corollary 14] With the present notation and considering*

- *the bilateral R-module $(\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^u$ with canonical basis $\{e_1, \ldots, e_u\}$,*
- *the bilateral Q-module $(Q \otimes_{\hat{R}} Q^{\mathrm{op}})^{|F|+m|G|}$ with canonical basis*

$$\{e_1, \ldots, e_u\} \sqcup \{\mathsf{e}_{ij\iota} : 1 \leq i < j \leq n, 1 \leq \iota \leq m\},$$

- *the projections $\mathfrak{S}_2 : (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^{|F|} \to \mathsf{R}^m : \mathfrak{S}_2(e_i) = g_i, 1 \leq i \leq u$, and*
- *$\hat{\mathfrak{S}}_2 : (Q \otimes_{\hat{R}} Q^{\mathrm{op}})^{|F|+m|C|} \to Q^m$:*

$$\hat{\mathfrak{S}}_2(e_i) = g_i, 1 \leq i \leq u, \quad \hat{\mathfrak{S}}_2(\mathsf{e}_{ij\iota}) = f_{ij\iota}, 1 \leq i < j \leq n, 1 \leq \iota \leq m,$$

- *the map*

$$\bar{\Pi} : (Q \otimes_{\hat{R}} Q^{\mathrm{op}})^{|F|+m|C|} \to (\mathsf{R} \otimes_{\hat{R}} \mathsf{R}^{\mathrm{op}})^{|F|}$$

(where each $\lambda, \rho \in R\langle Y_1, ..., Y_n\rangle, a, b \in R \setminus \{0\}$)

$$\bar{\Pi}\left(\sum_i a_i \lambda_i e_i b_i \rho_i + \sum_{ij\iota} a_{ij\iota} \lambda_{ij\iota} \mathsf{e}_{ij\iota} b_{ij\iota} \rho_{ij\iota}\right) = \sum_i a_i \Pi(\lambda_i) e_i b_i \Pi(\rho_i),$$

if $\Sigma \subset (Q \otimes_{\hat{R}} Q^{\mathrm{op}})^{|F|+m|C|}$ is a bilateral standard basis of $\ker(\hat{\mathfrak{S}}_2)$, then $\bar{\Pi}(\Sigma)$ is a bilateral standard basis of $\ker(\mathfrak{S}_2)$.

10 Lazard Structural Theorem for Ore Extensions over a Principal Ideal Domain

Let $\mathbb{D}$ be a commutative principal ideal domain, $\mathsf{R} := \mathbb{D}[Y; \alpha, \delta]$ be an Ore extension and $\mathsf{I} \subset \mathsf{R}$ be a bilateral ideal.

Let $F := \{f_0, f_1, \ldots, f_k\}$ be a reduced minimal strong bilateral Gröbner basis of I ordered so that

$$\deg(f_0) \leq \deg(f_1) \leq \cdots \leq \deg(f_k)$$

and let us denote, for each i, $c_i := \mathrm{lc}(f_i)$, $r_i \in \mathbb{D} \setminus \{0\}$ and $p_i \in \mathsf{R}$ the content[5] and the primitive part of f_i so that $f_i = r_i p_i$; denoting $P := p_0$ the primitive part of f_0 and $G_{k+1} := r_k \in \mathbb{D} \setminus \{0\}$ the content of f_k we have

Theorem 78. *With the present notation, for each $i, 0 < i \leq k$, there is $H_i \in \mathsf{R}, d(i) := \deg(H_i)$ and $G_i \in \mathbb{D} \setminus \{0\}$ such that*

[5] Defined here as the greatest common divisor of the coefficients of f_i in the principal ideal domain $\mathbb{D}$.

– $f_0 = G_1 \cdots G_{k+1} P$,

– $f_j = G_{j+1} \cdots G_{k+1} H_j P, 1 \leq j \leq k$,

and

1. $0 < d(1) < d(2) < \cdots < d(k)$;
2. $G_i \in \mathbb{D}, 1 \leq i \leq k+1$, *is such that* $c_{i-1} = G_i c_i$
3. $P = p_0$ *(the primitive part of* $f_0 \in \mathsf{R}$*);*
4. $H_i \in \mathsf{R}$ *is a monic polynomial of degree* $d(i)$*, for each* i*;*
5. $H_{i+1} \in (G_1 \cdots G_i, G_2 \cdots G_i H_1, \ldots, G_{j+1} \cdots G_i H_j, \ldots, G_i H_{i-1}, H_i)$ *for all* i.
6. $r_i = G_{i+1} \cdots G_{k+1}$.

Proof. Let P and G_{k+1} be, resp., the greatest common right divisor of $\{p_0, \ldots, p_k\}$ in R and the greatest common divisor of $\{r_0, \ldots, r_k\}$ in $\mathbb{D}$; since a set $\{g_0, \ldots, g_k\}$ is a minimal strong Gröbner basis if and only if the same is true for $\{rg_0 g, \ldots, rg_k g\}$, $r \in \mathbb{D}, g \in \mathsf{R}$, we can left divide by G_{k+1} and right divide by P and assume wlog that $P = G_{k+1} = 1$ and that both the greatest common right divisor of $\{p_0, \ldots, p_k\}$ and the greatest common divisor of $\{r_0, \ldots, r_k\}$ are 1.

Setting $\mathsf{d}(i) := \deg(f_i)$ and $\nu(i) := \mathsf{d}(i+1) - \mathsf{d}(i)$ for each i, by assumption we have $\mathsf{d}(i) \leq \mathsf{d}(i+1)$.

If $\mathsf{d}(i) = \mathsf{d}(i+1)$, let us define

$$h := b_i f_i + b_{i+1} f_{i+1} \in \mathsf{I}$$

where $c, b_i, b_{i+1} \in \mathbb{D}$ are such that $b_i c_i + b_{i+1} c_{i+1} = c$, c being the greatest common divisor of c_i and c_{i+1}, so that $cY^{\mathsf{d}(i+1)} = \mathbf{M}(h) \in \mathbf{M}(\mathsf{I})$; this implies the existence of j such that $\mathbf{M}(f_j) \mid \mathbf{M}(h) \mid \mathbf{M}(f_{i+1})$ contradicting minimality; thus $\mathsf{d}(i) < \mathsf{d}(i+1)$ and this, in turn, implies (1) since $d(i) = \mathsf{d}(i) - \deg(P)$.

Both $f_i Y^{\nu(i)}$ and f_{i+1} are in the ideal and have degree $\mathsf{d}(i+1)$.

Therefore, for $c, b_i, b_{i+1} \in \mathbb{D}$ such that $b_i c_i + b_{i+1} c_{i+1} = c$, c being the greatest common divisor of c_i and c_{i+1}, $h := b_i f_i Y^{\mathsf{d}(i+1)-\mathsf{d}(i)} + b_{i+1} f_{i+1} \in \mathsf{I}$, so that $cY^{\mathsf{d}(i+1)} = \mathbf{M}(h) \in \mathbf{M}(\mathsf{I})$ and $\mathbf{M}(f_j) \mid \mathbf{M}(h)$ for some j. If $c_{i+1} \neq c$, necessarily $\deg(f_j) < \deg(f_{i+1})$ whence $j < i+1$ and $\mathbf{M}(f_j) \mid \mathbf{M}(h) \mid \mathbf{M}(f_{i+1})$ getting a contradiction. As a conclusion $c_i = G_{i+1} c_{i+1}$, for some $G_{i+1} \in \mathbb{D}$ and (2).

Since $G_{i+1} f_{i+1} - f_i Y^{\nu(i)}$ is a polynomial of degree less than $\mathsf{d}(i+1)$ which reduces to zero by the Gröbner basis, it follows that

$$G_{i+1} f_{i+1} \in \mathbb{I}(f_0, \ldots, f_i) \text{ for each } i, 0 \leq i < k;$$

thus, inductively we obtain

$$p_0 \mid_R f_j \text{ for each } j \leq i \implies p_0 \mid_R f_j \text{ for each } j \leq i+1.$$

Also

$$\begin{aligned} c_i \mid_L f_j \text{ for each } j \le i \quad &\Longrightarrow \quad G_{i+1}c_{i+1} = c_i \mid_L G_{i+1}f_{i+1} \\ &\Longrightarrow \quad c_{i+1} \mid_L f_j \text{ for each } j \le i+1. \end{aligned}$$

Therefore, the assumptions that the greatest common right divisor of $\{p_0, \ldots, p_k\}$ and the greatest common divisor of $\{r_0, \ldots, r_k\}$ are 1 imply that $p_0 = c_k = 1$ proving (3); thus in particular $f_0 = c_0$ so that $c_0 \mid f_0$ and this is sufficient to deduce, by the inductive argument, that each c_i left-divides f_i and therefore coincides with r_i.

Inductively we obtain

$$r_i \operatorname{lc}(P) = c_i = G_{i+1}c_{i+1} = G_{i+1}r_{i+1} \operatorname{lc}(P) = G_{i+1} \cdots G_{k+1} \operatorname{lc}(P)$$

thus proving (6); defining H_i the polynomial s.t. $c_i H_i P = f_i$ for all i we have $\operatorname{lc}(H_i) = 1$ (proving (4)), $d(i) + \deg(P) = \deg(f_i)$ and $G_{i+1}f_{i+1} \in (f_0, \ldots, f_i)$ which proves (5) dividing out $G_{i+1} \cdots G_{k+1}$. □

A The PIR case

While an understandable *timor* restrained us to violate Ore's *tabu* requiring degree preservation of product, it is well-known that Zacharias–Möller results are naturally stated for polynomials over PIRs and the restriction to PIDs is unnatural; we therefore sketch here the few modifications to the theory which are required in order to adapt it to Ore extensions R over a PIR R.

The first delicate adaptation is required by formula (4); the natural solution is due to Gateva [16, 17, 18] who considered valuation over the semigroup with zero $\mathcal{T} \cup \{o\}$ instead of $\mathcal{T}$ setting

$$\circ : \mathbf{N} \times \mathbf{N} \to \mathbf{N} \cup \{o\} : u \circ v = \begin{cases} \mathbf{T}(u \star v) & u \star v \neq 0 \\ o & u \star v = 0. \end{cases}$$

Her theory however applies only to domains.

Thus in order to extend Corollary 15 we need to reformulate it as

Corollary 15. *If $\prec$ is a term ordering on $\mathcal{T}$ and $<$ is a $\prec$-compatible term ordering on $\mathcal{T}^{(m)}$, then, for each $l, r \in \mathsf{R}$ and $f \in \mathsf{R}^{(m)}$,*

1. $\mathbf{M}(l \star f) = \mathbf{M}(\mathbf{M}(l) \star \mathbf{M}(f))$ *provided* $\operatorname{lc}(l) \operatorname{lc}(f) \neq 0$*;*
2. $\mathbf{M}(f \star r) = \mathbf{M}(\mathbf{M}(f) \star \mathbf{M}(r))$ *provided* $\operatorname{lc}(f) \operatorname{lc}(r) \neq 0$*;*
3. $\mathbf{M}(l \star f \star r) = \mathbf{M}(\mathbf{M}(l) \star \mathbf{M}(f) \star \mathbf{M}(r))$ *provided* $\operatorname{lc}(l) \operatorname{lc}(f) \operatorname{lc}(r) \neq 0$.
4. $\mathbf{T}(l \star f) \le \mathbf{T}(l) \circ \mathbf{T}(f)$ *equality holding provided that* $\operatorname{lc}(l) \operatorname{lc}(f) \neq 0$*;*
5. $\mathbf{T}(f \star r) \le \mathbf{T}(f) \circ \mathbf{T}(r)$ *equality holding provided that* $\operatorname{lc}(f) \operatorname{lc}(r) \neq 0$*;*
6. $\mathbf{T}(l \star f \star r) \le \mathbf{T}(l) \circ \mathbf{T}(f) \circ \mathbf{T}(r)$ *equality holding provided that* $\operatorname{lc}(l) \operatorname{lc}(f) \operatorname{lc}(r) \neq 0$.

As regards Gröbner basis computation we remark that the first and the third algorithms (Section 6.1 and 6.3) apply *verbatim* also in the PIR case; in the algorithm in fact we have $\{i\} \in \mathfrak{H}(F)$ for each $i, 1 \leq i \leq u$ and thus each $\mathsf{m} := \mathbf{T}(g_i) \in \mathsf{T}$ is treated by the algorithm which (if the basis is minimal) produces also the annihilator syzygy

$$(d_1, \ldots, d_u) \in \mathrm{Syz}_L(v(\mathsf{m})_1, \ldots, v(\mathsf{m})_u), d_j := \begin{cases} a_j & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}$$

where we denote, for each $i \leq u$, $a_i \in R$ the annihilator of $\mathbb{I}(c_i)$.

In the second algorithm (Section 6.2) the inductive seed becomes

$$\mathcal{S}_1 = \{b \in R : b \operatorname{lc}(g_1) = 0\} = \mathbb{I}(a_1) \subset R,$$

and, for each $s, 1 < s \leq u$, $\{s\}$ is basic for $\mathbf{T}(g_s)$ provided the basis is minimal.

Therefore

Corollary 49. *Assuming that the Zacharias ring R is principal and denoting, for each $i, j, 1 \leq i < j \leq u$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,*

$$\begin{aligned}
b(i,j) &:= \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},j}(c_j)} \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_j} e_j \\
&- \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},i}(c_i)} \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_i} e_i, \\
B(i,j) &:= \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},j}(c_j)} \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_j} \star g_j \\
&- \frac{\operatorname{lcm}\left(\alpha_{\{i,j\},i}(c_i), \alpha_{\{i,j\},j}(c_j)\right)}{\alpha_{\{i,j\},i}(c_i)} \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_i} \star g_i \\
a(i) &:= a_i e_i \\
A(i) &:= a_i \star g_i,
\end{aligned}$$

we have that

$$\{b(i,j) : 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\} \cup \{a(i), i \leq u\}$$

is a left Gebauer–Möller set for F, so that F is a left Gröbner basis of M iff each $B(i,j)$, $1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$, and each $A(i), i \leq u$, have a left weak Gröbner representation in terms of F. □

Corollary 51. *Assuming that the Zacharias ring R is principal and that each α_i is an automorphism denoting, for each $i, j, 1 \leq i < j \leq u$, $\mathbf{e}_{l_i} = \mathbf{e}_{l_j}$,*

$$\begin{aligned}
b(i,j) &:= e_j \alpha_{\tau_j}^{-1}\left(\frac{\operatorname{lcm}(c_i, c_j)}{c_j}\right) \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_j} - e_i \alpha_{\tau_i}^{-1}\left(\frac{\operatorname{lcm}(c_i, c_j)}{c_i}\right) \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_i} \\
B(i,j) &:= g_j \star \alpha_{\tau_j}^{-1}\left(\frac{\operatorname{lcm}(c_i, c_j)}{c_j}\right) \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_j} - g_i \star \alpha_{\tau_i}^{-1}\left(\frac{\operatorname{lcm}(c_i, c_j)}{c_i}\right) \frac{\operatorname{lcm}(\tau_i, \tau_j)}{\tau_i} \\
a(i) &:= e_i \alpha_{\tau_i}^{-1}(a_i), \\
A(i) &:= g_i \star \alpha_{\tau_i}^{-1}(a_i),
\end{aligned}$$

we have that

$$\{b(i,j) : 1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}\} \cup \{a(i), i \leq u\}$$

is a right Gebauer–Möller set for F, so that F is a right Gröbner basis of M *iff each $B(i,j)$, $1 \leq i < j \leq u, \mathbf{e}_{l_i} = \mathbf{e}_{l_j}$, and each $A(i), i \leq u$, have a right weak Gröbner representation in terms of F.*

Proposition 54 (Möller)**.** *With the present notation and under the assumption that R is a principal ideal ring, the following conditions are equivalent:*

1. *F is a left Gröbner basis of* M*;*
2. *a completion of F is a strong left Gröbner basis of* M*.*

Buchberger's First Criterion, for the PIR case, is stated as

If $F \subset \mathcal{P}$ and $\mathbb{I}(F)$ is an ideal of $\mathcal{P}$, it holds

$$\begin{aligned} \mathbf{M}(i)\mathbf{M}(j) = \mathbf{M}(i,j) \quad &\Longleftrightarrow \quad \operatorname{lcm}(\tau_i, \tau_j) = \tau_i\tau_j, \operatorname{lcm}(c_i, c_j) = c_i c_j \\ &\Longrightarrow \quad \operatorname{NF}(B(i,j), F) = 0. \end{aligned}$$

Corollary 59. *With the present notation, under the assumption that R is a principal ideal ring, F is a left Gröbner basis of the left module* M *iff, denoting $\mathfrak{GM}$ a useful S-pair set for F, each S-polynomial $B(i,j), \{i,j\} \in \mathfrak{GM}$, and each $A(i), 1 \leq i \leq u$, have a left Gröbner representation in terms of F.*

Corollary 62. *With the present notation, under the assumption that R is a principal ideal ring, F is a left Gröbner basis of* M *iff each S-polynomial $B(i,j), \{i,j\} \in \mathfrak{R}$, and each $A(i), 1 \leq i \leq u$, has a left Gröbner representation in terms of F.*

Corollary 73. *With the present notation, under the assumption that R is a principal ideal ring, F is a restricted Gröbner basis of* M *iff*

1. *each S-polynomial $B_W(i,j), \{i,j\} \in \mathfrak{R}$, and each $A(i), 1 \leq i \leq u$, has a restricted Gröbner representation in terms of F;*
2. *for each $g_j \in F$, both $Y_i \star g_j, 1 \leq i \leq n$ and each $g_j \star \alpha_v(v), v \in \overline{\mathbf{v}}, v \in \mathcal{T}, v < \mathbf{T}(g_j)$, have a restricted representation in terms of F w.r.t. $<$.*

Finally we remark that a Lazard Structural Theorem for Ore Extensions over a Principal Ideal Domain can be easily obtained by adapting the result given by Norton–Sălăgean [36, 37], [31, § 33.3] for polynomial rings.

References

[1] Apel J., *Gröbnerbasen in Nichetkommutativen Algebren und ihre Anwendung*, Dissertation, Leipzig (1988)

[2] Apel J., *Computational ideal theory in finitely generated extension rings*, Theor. Comp. Sci. **224** (2000), 1–33

[3] Apel J., Lassner, W., *An Algorithm for calculations in enveloping fields of Lie algebras*, In: *Proc. Int. Conf. on Comp. Algebra and its Appl. n Theoretical Physics* JINR **D11-85-792**, Dubna (1985) 231–241

[4] Apel J., Lassner, W., *Computation and Simplification in Lie fields*, L. N. Comp. Sci. **378** (1987), 468–478, Springer

[5] Bergman G.H., *The Diamond Lemma for Ring Theory*, Adv. Math. **29** (1978), 178–218

[6] E. Byerne, *Gröbner bases over commutative rings and Applications to coding theory* in M. Sala et al. (Ed.) *Gröbner bases, Coding, Cryptography*, Springer Risc XVI, (2009). 239–262

[7] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Thesis, Innsbruck (1965)

[8] Buchberger B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem*, Aeq. Math. **4** (1970), 374–383

[9] Buchberger B., *A Critorion for Detecting Unnecessary Reduction in the Construction of Gröbner bases*, L. N. Comp. Sci **72** (1979), 3–21, Springer

[10] Buchberger B., *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in Bose N.K. (Ed.) *Multidimensional Systems Theory* (1985), 184–232, Reider

[11] J. Bueso, J. Gomez-Torrecillas, and A. Verschoren. *Methods in Non-Commutative Algebra* (2003). Kluwer

[12] Ceria, M., Mora, T. *Buchberger-Weispfenning Theory for Effective Associative Rings*, accepted by J. Symb. Comp., special issue for ISSAC 2015.

[13] Chyzak F., Salvy B. *Non-commutative Elimination in Ore Algebras Proves multivariate Identities* J. Symb. Comp. **26** (1998), 187–227

[14] Cohn P.M., *Noncommutative unique factorization domains* Trans. A.M.S. **109** (1963), 313–331

[15] Cohn P.M., *Ring with a week Algorithm* Trans. A.M.S. **109** (1963), 332–356

[16] Gateva–Ivanova T., *Groebner bases in skew polynomial rings*, J. Algebra **138** (1991) 13–35

[17] Gateva–Ivanova T., *Noetherian Properties of Skew Polynomial Rings with Binomial Relations*, Trans. A.M.S. **345** (1994), 203–219,

[18] Gateva–Ivanova T., *Skew polynomial rings with binomial relations*, J. Algebra **185** (1996) 710–753

[19] Gebauer R., Möller H.M., *On an Installation of Buchbgerger's Algorithm*, J. Symb. Comp. **6**, (1988), 275–286

[20] Janet M. , *Sur les systèmes d'équations aux dérivées partielles* J. Math. Pure et Appl., **3** (1920), 65–151

[21] Kandri-Rody A., Kapur, D. *Computing the Gröbner basis of an ideal in polynomail rings over a Euclidean ring* J. Symb. Comp. **6** (1990), 37–56

[22] Kandri-Rody, A., Weispfenning, W., *Non-commutativer Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9** (1990), 1–26

[23] Kredel, H. *Solvable Polynomial rings* Dissertation, Passau (1992)

[24] LaScala R., Levandovskyy V. *Skew Polynomial Rings, Gröbner bases and the Letterplace embedding of the free Associativ algebra*, J. Symb. Comp. **48** (2013), 110–131

[25] Lazard D., *Solving zero-dimensional algebraic systems* J. Symb. Comp. **15** (1992), 117–132

[26] Levandovskyy V. G., *Non-commutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementation*Dissertation, Kaiserslautern (2005)

`http://kluedo.ub.uni-kl.de/volltexte/2005/1883/`

[27] Levandovskyy V. G., *PBW Bases, Non-Degeneracy Conditions and Applications* In: Buchweitz, R.-O., Lenzing, H. (Eds.), *Representation of Algebras and Related Topics* (Proceedings of the ICRA X Conference),**45**. AMS. Fields Institute Communications,pp.229-246.

[28] Mansfield E.L.,Szanto A. *Elimination Theory for Differential Difference Polynomnials* Proc. ISSAC 2002 (2002), 283–290, ACM

[29] F. Mora, *De Nugis Groebnerialium 4: Zacharias, Spears, Möller* Proc. ISSAC'15 (2015), 191–198, ACM

[30] T. Mora, *Seven variations on standard bases*, (1988)

`ftp://ftp.disi.unige.it/person/MoraF/PUBLICATIONS/7Varietions.tar.gz`

[31] T. Mora *Solving Polynomial Equation Systems II: Macaulay's Paradigm and Gröbner Technology*, Cambridge University Press (2005)

[32] T. Mora *Zacharias Representeation of Effective Associative Rings*, J. Symb. Comp. (submitted)

[33] Mosteig E., Sweedler M. *Valuations and filtrations*, J. Symb. Comp. **34** (2002), 399–435

[34] Möller H.M., *New constructive methods in classical ideal theory*, J. Algebra **100** (1986) 138–178

[35] Möller H.M., *On the construction of Gröbner bases using syzygies*, J. Symb. Comp. **6** (1988), 345–359

[36] Norton G.H., Sălăgean A., *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. **64** (2001), 505–528

[37] Norton G.H., Sălăgean A., *Gröbner bases and products of coefficient rings*, Bull. Austral. Math. Soc. **65** (2002), 147–154

[38] Ore O., *Linear equations in non-commutative fields* , Ann. Math. **32** (1931), 463–477

[39] Ore O., *Theory of non-commutative polynomials* , Ann. Math. **34** (1933), 480–508.

[40] Pan L., *On the D-bases of polynomial ideals over principal ideal domains*, J. Symb. Comp. **7** (1988), 55–69

[41] Pesch M., *Gröbner Bases in Skew Polynomial Rings* Dissertation,Passau (1997)

[42] Pesch M., *Two-sided Gröbner bases in Iterated Ore Extensions*, Progress in Computer Science and Applied Logic **15** (1991), 225–243, Birkhäuser

[43] Pritchard F. L., *A syzygies approach to non-commutative Gröbner bases*, Preprint (1994)

[44] Pritchard F. L., *The ideal membership problem in non-commutative polynomial rings*, J. Symb. Comp. **22** (1996), 27–48

[45] Reinert B., *A systematic Study of Gröbner Basis Methods*, Habilitation, Kaiserslautern (2003)

[46] Reinert B., *Gröbner Bases in Function Ring – A Guide for Introducing Reduction Relations to Algebraic Structures*, J. Symb. Comp. **41** (2006), 1264–94

[47] Schreyer F.O., *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionsatz*, Diplomarbait, Hamburg (1980)

[48] Schreyer F.O., *A standard basis approach to syzygies of canonical curves*, J. Reine angew. Math. **421** (1991), 83–123

[49] Spear D.A., *A constructive approach to commutative ring theory*, in *Proc. of the 1977 MACSYMA Users' Conference*, NASA CP-2012 (1977), 369–376

[50] Sweedler M. *Ideal bases and valuation rings*, Manuscript (1986) available at
`http://math.usask.ca/fvk/Valth.html`

[51] Szekeres L., *A canonical basis for the ideals of a polynomial domain*, Am. Math. Monthly **59** (1952), 379–386

[52] Tamari D. *On a certain Classification of rings and semigroups* Bull. A.M.S. **54** (1948), 153–158

[53] Weispfenning, V. *Finite Gröbner bases in non-noetherian Skew Polynomial Rings* Proc. ISSAC'92 (1992), 320–332, A.C.M.

[54] Zacharias G., *Generalized Gröbner bases in commutative polynomial rings*, Bachelor's thesis, M.I.T. (1978)